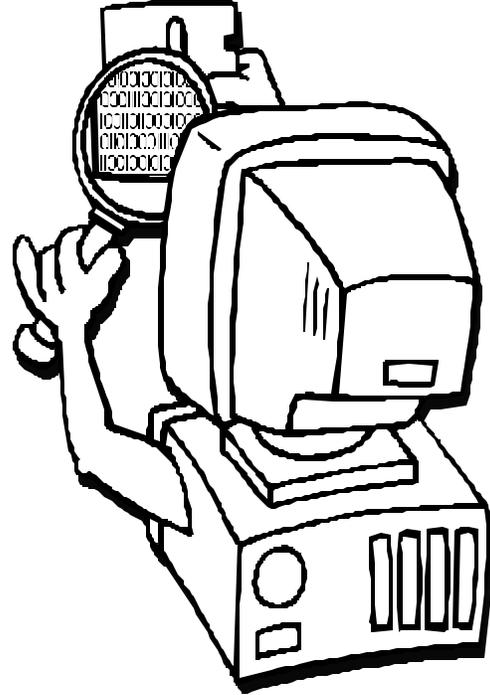

Aircraft Certification's New Software Policy



An Interactive Video Teletraining Course

Developed and Presented by

Leanna Rierson

Software Program Manager, AIR-130

Aircraft Engineering Division

Aircraft Certification Service

Federal Aviation Administration

April 28-29, 1999

CONTENTS OF IVT GUIDE

How Do I Use This IVT Guide?

IVT Course Orientation

What Is IVT?

Who Is the Target Audience?

Who Is the Instructor?

What Will You Learn?

What Does the Lesson Cover?

Appendices

- A. Software Policy Presentation Visuals
- B. N8110.81 – Software Review Notice
- C. N8110.77 – Field-Loadable Software Notice
- D. N8110.79 – PMA for FLS Notice
- E. N8110.84 – User-Modifiable Software Notice
- F. N8110.78 – Legacy Systems Notice
- G. N8110.82 – Level D and Previously Developed
Software Notice
- H. N8110.83 – Software Tool Qualification Notice
- I. Evaluation Form

**How Do I Use
This IVT
Guide?**

This Interactive Video Teletraining (IVT) Guide provides you with an orientation to the IVT presentation, support materials for use during the broadcast, and the course evaluation.

Follow these steps to complete your study.

1. Review the *IVT Presentation Orientation* before the broadcast, if possible, or before you watch the self-study videotape. It provides the purpose of the presentation, the target audience, information about the instructor, what you will learn, and topics covered.
2. Turn to Appendix A, *IVT Presentation Visuals*, and refer to it during the broadcast/videotape. You can use these visuals to take notes and follow along when viewing the presentation/self-study video.
3. Review the software notices in Appendices B-H before the broadcast, if possible, or before you watch the self-study videotape.
4. Complete the *IVT Presentation Evaluation Form* in Appendix I and send it to your Directorate/Division Training Manager (ATM). Your comments are very important to us and will help to enhance the quality of the IVT lesson.

NOTE: The IVT broadcast will be videotaped so that it may be used as a self-study package for those who were unable to participate in the broadcast, or for those who wish to refresh their knowledge of the content presented. This IVT Guide may also be used with the self-study videotape.

What Is IVT?

Interactive Video Teletraining, or IVT, is instruction delivered using some form of live, interactive television. This course originates from the television studio at the FAA Academy in Oklahoma City. Through the IVT broadcast facility, the instructor is able to use a variety of visuals, objects, and media formats to support the instruction.

Participants are located at various receive sites around the country and can see the instructor and his/her materials on television sets in their classrooms. The participants can communicate with the instructor either through a microphone and/or the simple-to-use Viewer Response System keypads. During the live presentation, when a participant has a question or the instructor asks for specific participant responses to questions, the participant(s) can signal to the instructor using the keypad.

The collective participant responses, or the name of a specific participant signaling a question, are immediately visible to the instructor on the console at the broadcast site. The instructor can then respond as needed. When the instructor calls on a specific participant to speak from a site, participants at each of the other sites can simultaneously hear the participant who is speaking.

This guide provides you with a framework for this course as well as the following three appendices to be used during the course:

- Appendix A contains copies of the actual slides used by the instructor during the broadcast. You can use these visuals to follow along with the broadcast or when you watch the tape and to record notes directly on the pages.
- Appendices B-H contain the Software Notices that will be discussed throughout the broadcast.
- Appendix I contains the IVT Course Evaluation Form. Please fill out this form after the IVT/self study course is finished and send the form to your Directorate/Division Training Manager (ATM).

Who Is the Target Audience?
Who Is the Instructor?

- Engineers who are responsible for approving software.

Leanna Rierson is the Software Program Manager for the Aircraft Certification Avionics Branch. She has ten years of experience in numerous computer/aviation industry positions. These positions include: avionics/electrical engineering specialist at the Wichita ACO and software positions with industry at NCR and Cessna Aircraft Company. Leanna graduated summa cum laude from Wichita State University and is currently working on a Master's and PhD degrees in Software Engineering.

What Will You Learn?

- At the end of the training, participants will be able to:
- Describe the purpose and content of the seven new software notices.
 - Explain the software review process.
 - Describe procedures for approving software in legacy systems.
 - Explain field-loadable software and user-modifiable software policy.
 - Describe software tool qualification.
 - Explain future software policy plans.

What Does the Presentation Cover?

The following outline gives an overview of the course content. In addition, Appendix A, contains all presentation slides.

- Topic 1: Introduction
- Topic 2: Software Review Process (N8110.81)
- Topic 3: Field-Loadable Software (N8110.77 & N8110.79)
- Topic 4: User-Modifiable Software (N8110.84)
- Topic 5: Software Changes to Legacy Systems (N8110.78)
- Topic 6: Level D and Previously Developed Software (N8110.82)
- Topic 7: Software Tool Qualification (N8110.83)
- Topic 8: Future Software Policy and Guidance
- Topic 9: Summary

Self-Assessment

Pre- & Post-Course Self-Assessment Questions

If you are taking this course via IVT and you are logged on to a keypad, you will be asked before and after the broadcast to complete this self assessment, using your keypads. If you are taking this via self-study video, please complete manually and return with your end of course evaluation to your directorate/division training manager (ATM).

Rate your confidence level for each of the following statements before and after completing the course.

1. I can explain the purpose of software policy.

	<u>Very Confident</u>	<u>Moderately Confident</u>	<u>Not Confident</u>
BEFORE THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AFTER THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. I can describe the current policy on field loadable software and user modifiable software.

	<u>Very Confident</u>	<u>Moderately Confident</u>	<u>Not Confident</u>
BEFORE THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AFTER THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. I can explain the FAA policy on the software review process.

	<u>Very Confident</u>	<u>Moderately Confident</u>	<u>Not Confident</u>
BEFORE THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AFTER THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. I can describe approval software changes to legacy systems, previously developed software, and software tool qualification.

	<u>Very Confident</u>	<u>Moderately Confident</u>	<u>Not Confident</u>
BEFORE THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AFTER THE COURSE:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Presentation Visuals

Appendix A

NOTES:

Aircraft Certification's New Software Policy

Leanna Rierson

Ph: 202-267-3785

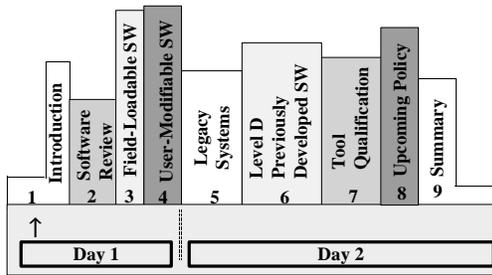
Fx: 202-493-5173

E-Mail: Leanna.Rierson@faa.gov

IVT Hotline: (888) 279-8604

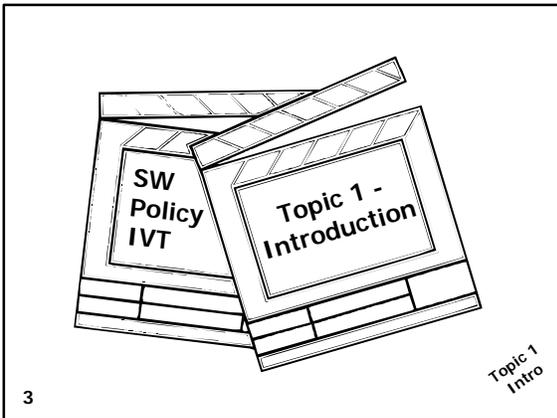
1

Course Overview



2

Software Policy Bookshelf



3

Topic 1
Intro

Course Objectives

- Describe The Purpose And Content Of The Seven New Software Notices
 - Explain The Software Review Process
 - Describe Procedures For Approving Software In Legacy Systems
 - Explain Field-Loadable Software And User- Modifiable Software Policy
 - Describe Software Tool Qualification
- Explain Future Software Policy Plans

Topic 1
Intro

4

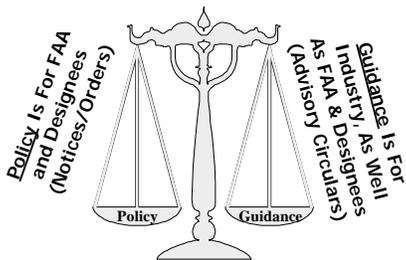
Background Information

- Software Grand Design Team Identified AIR's Software Policy and Guidance Needs
- Seven Notices Have Been Completed
- Four Notices Are In Progress
- Software Notices Will Be Combined Into A Single Software Order
- One Guidance Area Was Identified -- Production Software Guidance

Topic 1
Intro

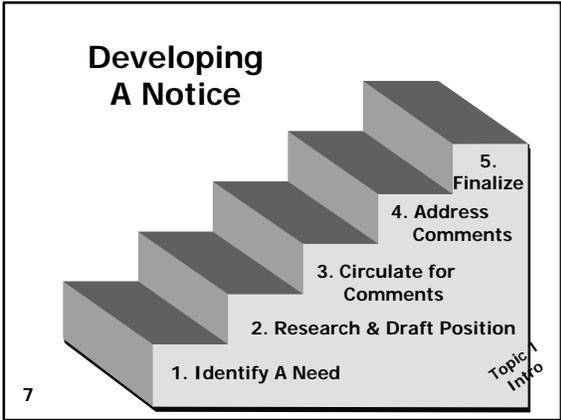
5

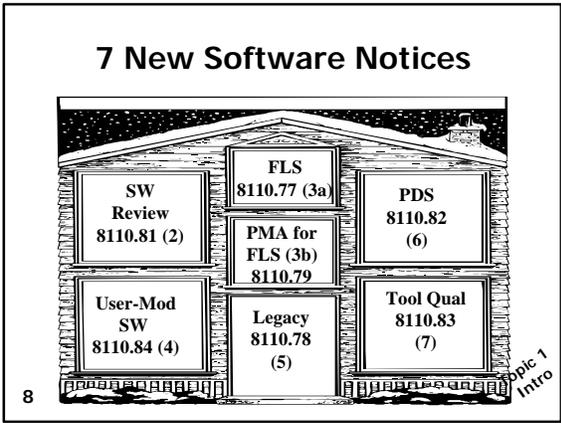
Policy vs. Guidance



Topic 1
Intro

6





- ### Ordering of Information For Each Topic
- Purpose And History
 - Technical Information
 - Notice Outline
 - Highlights Of Notice
 - Summary
- 9
- Topic 1
Intro



Topic 2

N8110.81 - Software Review Process

10

*Topic 2
N8110.81*

Purpose and History

- **Purpose:**
 - Provides Guidelines to Certification Authorities for Performing Software Reviews
 - Clarifies Software Review Process Discussed in DO-178B
 - Standardizes the Review Approach, As Detailed in the Software Job Aid

11

*Topic 2
N8110.81*

Purpose and History

- **History:**
 - Began - 1996
 - Modified - 1998
 - Job Aid and IVT, "Conducting Software Reviews Prior to Certification" - 1998
 - Finalized - March 1999

12

*Topic 2
N8110.81*

Technical Information

- Relationship to DO-178B
 - Section 9.2 and 10.3
- Relationship to Software Job Aid
 - N8110.81 is “WHAT” Document
 - Job Aid is “HOW” Document
 - N8110.81 is Policy
 - Job Aid is a Training Tool



Topic 2
N8110.81
13

N8110.81 Outline

- Sections 1-3: Purpose, Distribution, Related Publications
- Section 4: Definitions
- Section 5: Scope
- Section 6: Objectives of Software Review Process
- Section 7: SW Review Process and Life Cycles
- Section 8: Additional Considerations
- Section 9: Preparing, Conducting, Documenting
- Section 10: Conclusion

Topic 2
N8110.81

14

Def: Review (Section 4) - 1/2

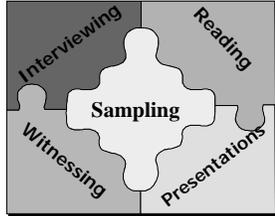


- Process of Examining Software Life Cycle Data, Project Records, and Other Evidence to Determine if DO-178B Objectives are Satisfied

Topic 2
N8110.81

15

Def: Review (Section 4) - 2/2
Typical Review Activities



16

Topic 2
Ns110.81

Def: Sampling (Section 4)

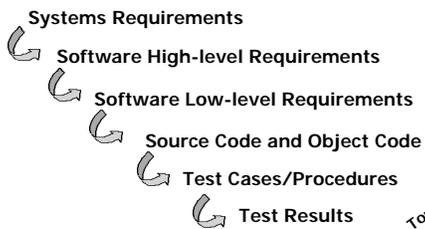
- Technique Used in Software Review
- Select Representative Software Life Cycle Data to Analyze Compliance to DO-178B Objectives

17

Topic 2
Ns110.81

Examples of Sampling - 1/2

- TRACEABILITY EXAMINATION



18

Topic 2
Ns110.81

Examples of Sampling - 2/2

- Review Safety Assessment Tie to Software Level
- Examine Structural Coverage Analysis
- Examine Software Quality Assurance and Configuration Management Records

19

Topic 2
NB110.81

Def: Presentation (Section 4)



- Applicant's Overview of the Software Program
- Used Sparingly During the Software Review Process
- May Not Give Full Picture of Actual Life Cycle Activities

20

Topic 2
NB110.81

Def: Findings and Observations (Section 4)

- Finding = Identification of a Failure to Meet DO-178B Objective(s)
- Observation = Identification of Potential Life Cycle Improvement

21

Topic 2
NB110.81

Scope (Section 5)

- DO-178B Discusses Certification Liaison Process (Section 9)
- DO-178B Address the Software Review by Certification Authorities (Section 9.2 and 10.3)

22

Topic 2
NB110.81

Scope (Section 5) Two Review Techniques



On-site



Desk

23

Topic 2
NB110.81

Scope (Section 5b) Making Arrangements

- Determine Type of Review (I.e., Planning, Development, Verification, or Final)
- Determine Dates, Locations, Personnel
- Determine Designee Involvement
- Specify Data to be Reviewed

24

Topic 2
NB110.81

Engineers & Inspectors Working Together



Job Aid and Future Policy Identifies Roles of Engineers and Inspectors

25

Topic 2
N8110.81

Purpose of Software Review (Section 6a)

- Address Technical Issues In A Timely Manner
- Examine Compliance Data -- Visibility
- Verify Adherence to Plans and Procedures
- Monitor Designees

26

Topic 2
N8110.81

Determine Level of FAA Involvement (LOFI) (Section 6b)

- Determine LOFI Early in the Project
- Determine When and How Many Reviews the FAA Will Perform
- LOFI Criteria Will Be Documented in a Notice
- LOFI Should Be Documented for Each Software Project

27

Topic 2
N8110.81

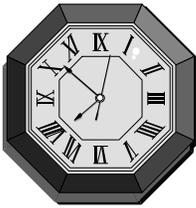
Examples of Levels of FAA Involvement (Section 6b)

- **High:** Critical System, Little DER Support, New to DO-178B (3-4 reviews)
- **Medium:** Critical System, Experienced DERs, Experience with DO-178B, A Few Novel Concepts (2-3 reviews)
- **Low:** Level D System, Good DER Support (0-1 review)

28

Topic 2
Ns110.81

Review Process & Life Cycles (Section 7)

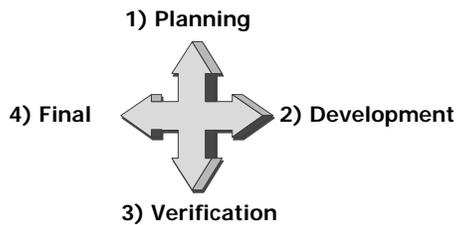


- **Reviews Should Begin Early in the Software Life Cycle**

29

Topic 2
Ns110.81

Four Types of Software Reviews (Section 7)



Note: In Job Aid These Were Called Stages of Involvement #1,2,3,4

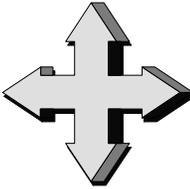
30

Topic 2
Ns110.81

Four Types of SW Reviews & Relationship to DO-178B - (Section 7)

1) Planning (A-1/A-8/A-9/A-10)

4) Final
(All)



2) Development
(A-2/A-3/A-4/
A-5/ A-6/A-8/
A-9/A-10)

3) Verification
(A-7/A-8/A-9/A-10)

31 Topic 2
Ns110.81

1. Software Planning Review (Section 7) - 1/2 

- Called "Stage of Involvement #1" in Job Aid
- Occurs When Applicant Has Completed Planning Life Cycle
- Typically Occurs:
 - When Plans/Standards Have Been Completed and Placed Under Change Control, and
 - After Applicant's QA Review of Plans

32 Topic 2
Ns110.81

1. Software Planning Review (Section 7) - 2/2

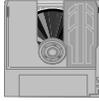
- Data To Review - See Table 1
- Review Data to Assess Compliance to the Following DO-178B Objectives:
 - Table A-1: All Objectives
 - Table A-8: Objectives 1-4
 - Table A-9: Objective 1
 - Table A-10: Objectives 1-2



33 Topic 2
Ns110.81

2. Software Development Review

(Section 7) - 1/3



- Called "Stage of Involvement #2" in Job Aid
- Occurs When Applicant is Well into Development Process
- Some Test Cases May Already be Started

34

Topic 2
Ns110.81

2. Software Development Review

(Section 7) - 2/3

- Criteria to Determine Readiness/Maturity of the Project for Review:
 - High-level Requirements are Complete and Trace to Systems Requirements
 - Software Architecture is Complete
 - Low-level Requirements are Complete and Trace to High-level Requirements
 - Source Code is Complete and Traces to Low-Level Requirements

35

Topic 2
Ns110.81

2. Software Development Review

(Section 7) - 3/3

- Data To Review - See Table 2
- Review Data to Assess Compliance to DO-178B Objectives:
 - Table A-2: Objectives 1-6
 - Table A-3 & A-4: All Objectives
 - Table A-5: Objectives 1-6
 - Table A-8: Objectives 1-4, 6
 - Table A-9: Objectives 1-2
 - Table A-10: Objective 3



36

Topic 2
Ns110.81



3. Software Verification Review

(Section 7) - 1/3

- Called "Stage of Involvement #3" in Job Aid
- Occurs When Applicant is Well into Verification/Test Process
- Assesses:
 - Implementation of Applicant's Verification Plans;
 - Completion of QA & CM Tasks;
 - Verification of Development Activities; and
 - Structural Coverage Analysis (if required)

37

Topic 2
NB110.81

3. Software Verification Review

(Section 7) - 2/3

- Criteria to Determine Readiness/ Maturity of the Project for Review:
 - Development Data is Complete and Under Configuration Control
 - Test Cases and Procedures are Documented, Reviewed, and Under Configuration Control
 - Testing is Completed or Well Under Way
 - Test Results are Documented, Per Plan
 - Testing Environment is Documented and Controlled

38

Topic 2
NB110.81

3. Software Verification Review

(Section 7) - 3/3

- Data To Review - See Table 3
- Review Data to Assess Compliance to DO-178B Objectives:
 - Table A-1: Objective 3
 - Table A-5: Objectives 7
 - Tables A-6, A-7, and A-8: All Objectives
 - Table A-9: Objectives 1-2
 - Table A-10: Objective 3

39

Topic 2
NB110.81

**4. Final Certification
Software Review**
(Section 7) - 1/3



- Called "Stage of Involvement #4" in Job Aid
- Address All Open Items
- Assure Compliance to All DO-178B Objectives

40

Topic 2
Ns110.81

**4. Final Certification
Software Review** (Section 7) - 2/3

- Occurs When:
 - Software Conformity Review Completed
 - Software Accomplishment Summary and Configuration Index Completed
 - All Software Life Cycle Data Completed and Placed Under Configuration Control

41

Topic 2
Ns110.81

**4. Final Certification
Software Review** (Section 7) - 3/3

- Data To Review - See Table 4
- Review Data to Assess Compliance to All DO-178B Objectives
- Assure That All Problem Reports, Action Items, and Certification Issues Have Been Addressed



42

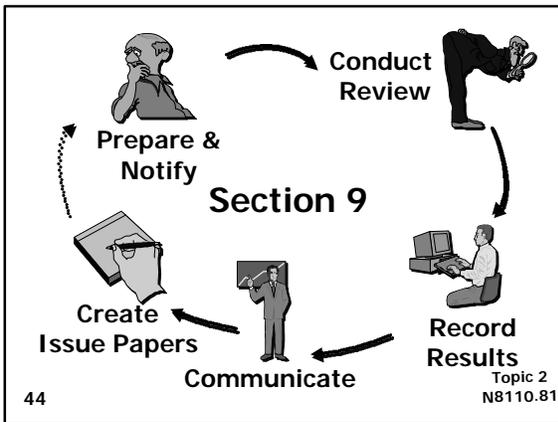
Topic 2
Ns110.81

Additional Considerations (Section 8)

- Number, Type, and Depth of Reviews May Vary Depending On:
 - Software Level
 - Product Attributes (size, complexity, ...)
 - New Technology or Unusual Design
 - Experience with DO-178B
 - Experience with Certification
 - Special Considerations
 - Designee Support

43

Topic 2
N8110.81



44

Topic 2
N8110.81

For Additional Information on Software Reviews

- Reference the Software Review Job Aid
- View the Video Training on Using the Software Review Job Aid
- Attend Software Fundamentals Course
- Attend Software Job Function Course (Only For SW Specialists)

45

Topic 2
N8110.81

Summary

- Provides Guidelines to Prepare, Conduct, and Document Software Reviews
- Formalizes Job Aid Information
- Outlines 4 Types of Reviews:
 - Planning, Development, Verification, Final

46

Topic 2
N8110.81



Topic 3

Field-Loadable Software N8110.77 and N8110.79

47

Topic 3

Two Field-Loadable Notices

- **N8110.77** - "Guidelines for the Approval of Field-Loadable Software"
- **N8110.79** - "Guidelines for Approval of Field Loadable Software by Finding Identity through the Parts Manufacturer Approval Process"

48

Topic 3

Purpose & History - 1/2

- **Purpose:**
 - To Provide Guidelines for Approving Field-Loadable Software (FLS)
 - To Clarify DO-178B FLS Guidance

49

Topic 3
N8110.77

Purpose & History - 2/2

- **History**
 - ACSEP Evaluation - May 1997
 - FLS Guidance Unclear
 - PMA Policy Did Not Specifically Address Software
 - Notice Drafted to Address FLS and PMA
 - Notice Routed for Comment - Jan. 1998
 - Comments Indicated Need for 2 Notices ⇒ N8110.77 and N8110.79

50

Topic 3
N8110.77

Notice Outline

- Section 1: Purpose
- Section 2: Distribution
- Section 3: Related Publications
- Section 4: Definitions
- Section 5: Background
- Section 6: Earlier Versions of DO-178
- Section 7: Approval Information
- Section 8: Installation Information
- Section 9: Maintenance and Part Marking

51

Topic 3
N8110.77

Definitions (Section 4)

Field-Loadable Software	Software that can be loaded without removal of the equipment from the aircraft installation.
User-Modifiable Software	Software intended for modification by the airplane operator without review by the certification authority, airframer, or equipment manufacturer.
Option-Selectable Software	Software that contains approved and validated components that may be activated by the user.

52

Topic 3
NB110.77

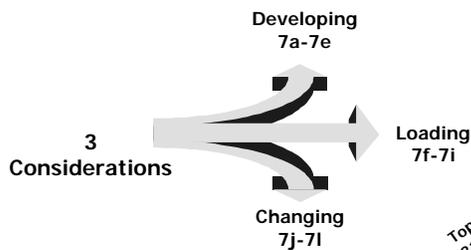
Examples (Section 4)

- **Field-Loadable Software**
 - Engine Control Software
 - Flight Control Software
 - Boeing 777 Has Many Systems With FLS
- **User-Modifiable Software**
 - Electronic Checklist
- **Option-Selectable Software**
 - Selection Of Sensors For An FMS

53

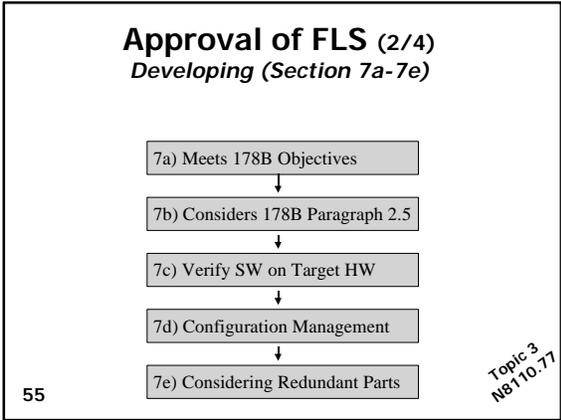
Topic 3
NB110.77

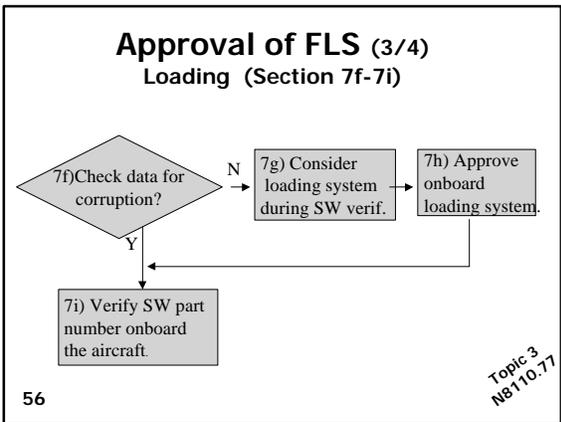
Approval of FLS (Section 7) - 1/4

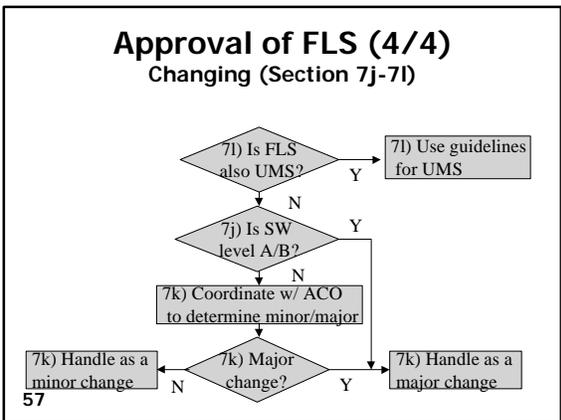


54

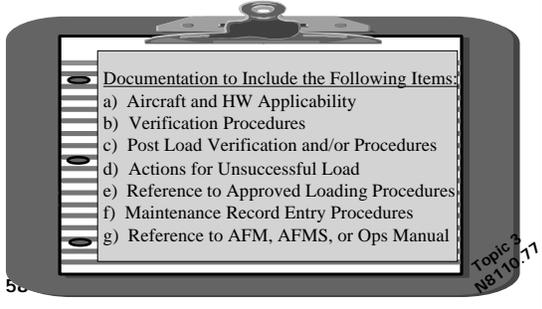
Topic 3
NB110.77







Installation of FLS (Section 8)



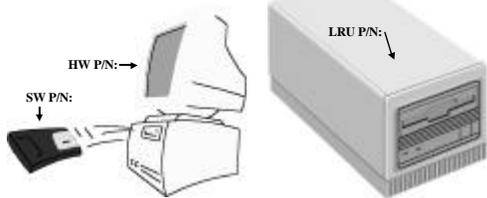
Maintenance & Part Marking of FLS (Section 9) - 1/2

- 9a) Procedure in AMM or IFCA for Maintenance
- 9b) Procedure to Include Reading of SW Version
- 9c) Procedure to Include P/N in Maintenance Records
- 9f) Changes Reflected in Appropriate Manual

59

Topic 3
N8110.77

Maintenance & Part Marking of FLS (Section 9) - 2/2

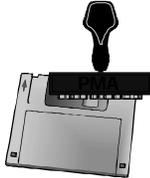


9d) Procedure to Verify SW Load

9e) Procedure to Verify Nameplate & SW Load

60

Parts Manufacturer Approval of Field-Loadable Software N8110.79



61

Topic 3
N8110.79

Purpose and History

- **PURPOSE:**
 - Provides Guidelines for Approving FLS Through PMA
 - Limited to Identity With or Without a Licensing Agreement
 - Does Not Cover Test and Computation

- **HISTORY**
 - Started As Part of N8110.77 But Was Separated For Clarity

62

Topic 3
N8110.79

Technical Information

- FLS Is Beneficial to Airlines and Applicants
- Order 8110.42, "PMA Procedures," Does Not Specifically Address Software
- CFRs 21.301, 303, and 305 Do Not Specifically Address Software
- Data Being Loaded Is Approved, Not Media

63

Topic 3
N8110.79

Procedures (Section 5) - 1/2

- Follow Part 21 and Order 8110.42 in Conjunction With the Software-Specific Procedures in N8110.79

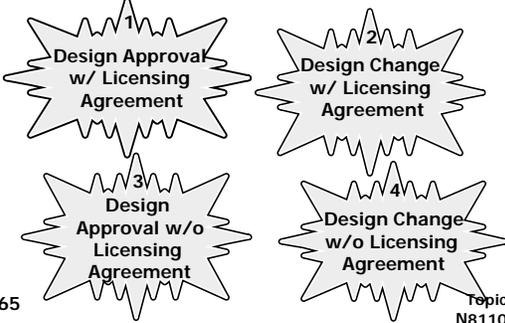


64

Topic 3
N8110.79

Procedures (Section 5) - 2/2

4 Situations For Identity Approval



65

Topic 3
N8110.79

Design Approval: Identity with Licensing Agreement (Section 5b(1)a)

- Reference 8110.42, 8(a)(3)(a)
- FLS Should Be Approved Through TC, STC, ATC as Described in N8110.77
- FLS Should Be Installed Via Service Bulletin Or Similar Means
- Configuration Management Process Should Be In Place To Assure Software P/N, Hardware P/N, Aircraft Series, etc. Are Accurate

66

Topic 3
N8110.79

Design Change: Identity with Licensing Agreement (Section 5b(1)b)

- Reference 8110.42, 8(h)(5)
- Applicant Should Coordinate Change With TC, STC, ATC Holder
- Determine Minor/Major Classification
 - Major change ⇒ 8110.42 8(h)(5)(a)
 - Minor change ⇒ 8110.42 8(h)(5)

67

Topic 3
NB110.79

Design Approval: Identity w/o Licensing Agreement (Section 5b(2)a)

- Order 8110.42, 8(a)(3)(b) - Parts Must Be Identical In "All Respects"
- FLS Should Be Identical To The Software On The TC, STC, ATC Approval
 - Bit-by-bit Comparison
 - Evidence of Identical Type Design Data - DO-178B Section 9.4

68

Topic 3
NB110.79

Design Change: Identity w/o Licensing Agreement (Section 5a(2)b)

- Change Considered Major
- Reference 8110.42, 8(h)(5)(a)

69

Topic 3
NB110.79

Summary

- **Two Notices Related to FLS**
 - N8110.77 - Guidelines for Approval of FLS
 - N8110.79 - Guidelines for PMA via Identity for FLS
 - Reference DO-178B, Part 21, and Order 8110.42

70

Topic 3



Topic 4

N8110.84 - Approval of Airborne Systems and Equipment Containing User-Modifiable Software

71

Topic 4
N8110.84

Purpose & History

- **PURPOSE**
 - To Provide Guidelines To ACO Engineers and DERs For Approval of Systems With User-Modifiable Software (UMS)
 - To Encourage Working With Flight Standards Personnel:
 - Maintenance Inspectors, Avionics Inspectors, and Operations Inspectors
- **HISTORY**
 - Started - 1996

72

Topic 4
N8110.84

Technical Information

Biggest Concerns:

- ✖ Corruption of Non-modifiable, Safety-related Software
- ✖ Change Control Problems in the Field
- ✖ Compelling but Invalid Information in the Cockpit

73

Topic 4
NB110.84

Notice Outline - 1/2

- Sections 1-3: Purpose, Distribution, Related Publications
- Section 4: Definitions
- Section 5: Scope
- Section 6: Earlier Versions of DO-178
- Section 7: Safety Considerations
- Section 8: Displayed Data
- Section 9: Aircraft Performance Parameters
- 74 • Section 10: Protection

Topic 4
NB110.84

Notice Outline - 2/2

- Section 11: Tools
- Section 12: Data Requirements
- Section 13: Other Considerations
- Section 14: Conclusion

75

Topic 4
NB110.84

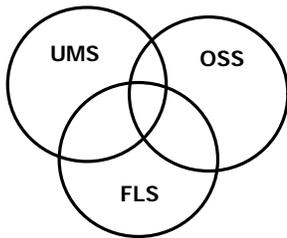
Definitions (Section 4) - 1/2

User-Modifiable Software	Software intended for modification by the airplane operator without review by the certification authority, airframer, or equipment manufacturer.
Option-Selectable Software	Software that contains approved and validated components that may be activated by the user.
Field-Loadable Software	Software that can be loaded without removal of the equipment from the aircraft installation.

76

Topic 4
NB110.84

Definitions (Section 4) - 2/2



77

Topic 4
NB110.84

Databases, etc?

- What About Navigation or Terrain Databases?
- What About Programmable Waypoints or Other Programmable Database-Like Items?

78

Topic 4
NB110.84

Scope (Section 5)

Notice is for User-Modifiable Software Only

79

Topic 4
NB110.84

Earlier Version of DO-178 (Section 6)

- Earlier Versions of DO-178 Contain No Guidance for User-Modifiable Software
- Use DO-178B Guidance for The User-Modifiable Portions

80

Topic 4
NB110.84

Safety Considerations (Section 7) - 1/3

- Once Certified as UMS There is No Certification Authority Oversight



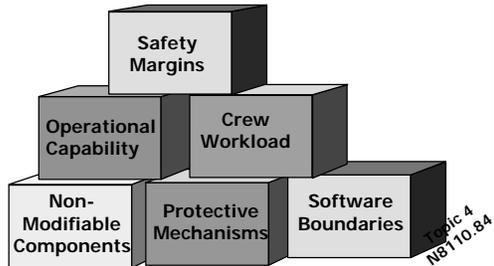
81

Topic 4
NB110.84

Safety Considerations

(Section 7) - 2/3

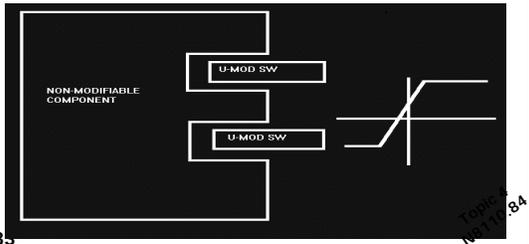
Modifications Should Have No Effect On



Safety Considerations

(Section 7) - 3/3

- Effects Must Be Bounded



Identification of Displayed Data (Section 8)



- Obvious or Explicit Indication That the Data is Not Cert Authority Approved

84

Topic 4
NB110.84

Performance Parameters
(Section 9) - 1/2

- **Modifications to Provide or Revise Performance Parameters Requires Certification Authority Review and Approval**
- **Examples of Parameters**
 - Safety margins
 - Operational capabilities
 - Crew workload

85

Topic 4
NB110.84

Performance Parameters
(Section 9) - 2/2

- **Changing Data To Determine Aircraft Performance Parameters = Major Change**



- **User-Modifiable Designation Lost**

86

Topic 4
NB110.84

Protection (Section 10) - 1/4

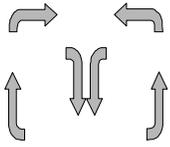
- **UMS Components Shouldn't Affect Non-UMS Components**
- **Assure Protection Is Developed to at Least Same Level of Robustness Required of the Most Robust Non-UMS Component**

87

Topic 4
NB110.84

Protection (Section 10) - 2/4

- Two Considerations
 - Operating In:
 - Protection in the design and operation
 - Changing Out:
 - Protection during modification



Topic 4
Ns110.84

88

Protection (Section 10) - 3/4

- **Examples**
 - Partitioning
 - Hardware Modes
 - Encoding
 - Tools
 - Modifications
 - Loading Protection

Topic 4
Ns110.84

89

Protection (Section 10) - 4/4



- Accidental Breach
 - Low Likelihood Under Reasonably Probable Circumstances
 - (This is a subjective statement of probability - not a xx.1309 definition)
- Intentional Breach
 - Low Likelihood Without Undue Effort

Protect Against Breaches

Topic 4
Ns110.84

90

Tools (Section 11) - 1/4



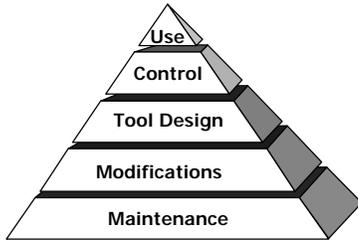
- Used to Enforce Protection
 - Not DO-178B Dev/Verif Tools
- Demonstrate As the Only Means To Modify UMS Component

Topic 4
NB110.84

91

Tools (Section 11) - 2/4

Requires Review and Approval Of:



Topic 4
NB110.84

92

Tools (Section 11) - 3/4

Design Approval of Tools



By ACO Engineer

Topic 4
NB110.84

93

Tools (Section 11) - 4/4

Maintenance Approval of Tools

Jointly By:

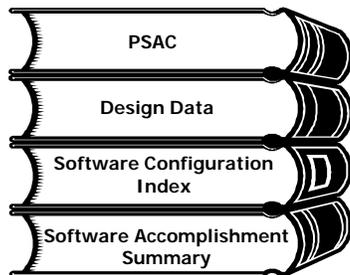
- ACO Engineer
- Operational Authority
- Maintenance Authority



94

Topic 4
NB110.84

Data Requirements (Section 12)



95

Topic 4
NB110.84

Other Considerations

(Section 13)

- User Follows the Approved Procedures for Modifications to UMS
- User Responsible for Configuration Management, Quality Assurance, and Verification of the Software
- Changing Anything Besides UMS Can Result in Certificate Being Rescinded

96

Topic 4
NB110.84

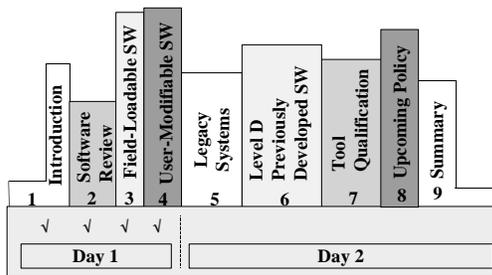
Summary

- N8110.84 Provides Guidelines For Approval of Systems & Equipment Containing UMS
- Provides Guidelines On
 - Safety Considerations
 - Safety Parameters
 - Protection
 - Tools
 - Data Requirements
 - Working With FSDO Personnel

97

Topic 4
N8110.84

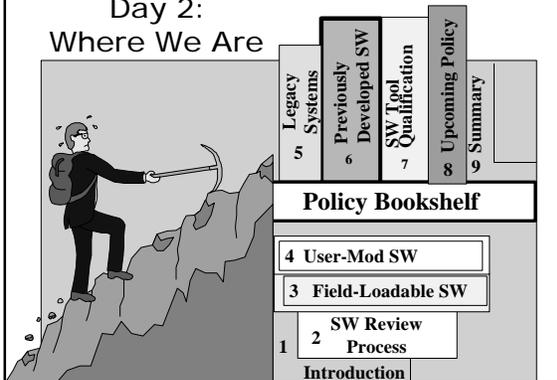
Where We Are

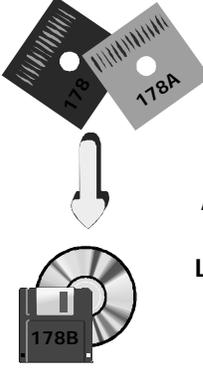


98

Software Policy Bookshelf

Day 2: Where We Are





Topic 5

Approval of Software Changes in Legacy Systems Using DO-178B N8110.78

100

*Topic 5
N8110.78*

Purpose & History - 1/2

- **Purpose:**
 - Provide Guidelines for Transitioning From DO-178/178A To DO-178B



101

*Topic 5
N8110.78*

Purpose & History - 2/2

- **History:**
 - Notice N8110.53 - 1994
 - N8110.53 Was Confusing To Many
 - Legacy Notice Written to Clarify
 - Legacy Notice Routed For Comments - March 1998
 - Legacy Notice Completed - Oct 1998

102

*Topic 5
N8110.78*

Technical Information

- Legacy System Is a System Whose Software Was Approved Prior to Issuance of DO-178B
- Legacy System Already Has a TC, STC, ATC, TSO, PC, and/or PMA Approval
- Legacy System Specifically Applies to Systems That Had Software Approved Using DO-178 or DO-178A

103

Topic 5
NB110.78

Technical Information Example of Legacy Systems

- Nav Unit Approved Using DO-178A and Originally Installed on a Citation II
- Installation of That Same Nav Unit Onto a Citation V, Learjet 45, or Raytheon Premiere → Legacy Systems
- Basically--Legacy Systems Concerns Arise Anytime a DO-178 or DO-178A System is Considered for Installation Onto an Aircraft or Engine

104

Topic 5
NB110.78

Notice Outline

- Section 1: Purpose
- Section 2: Distribution
- Section 3: Related Publications
- Section 4: Background
- Section 5: Discussion
- Section 6: Procedures
- Section 7: Conclusions

105

Topic 5
NB110.78

Background (Section 4) - 1/2

- Comparison of DO-178B to DO-178/178A
 - DO-178B Hinges on Objectives Rather Than Goal Statements
 - Software Testing is More Thorough in DO-178B
 - Software Level Classification Differs
 - (5 levels vs. 3 levels)
 - Tool Qualification Addressed in DO-178B

106

Topic 5
NB110.78

Background (Section 4) - 2/2

- Since AC 20-115B “cancels” DO-178A and DO-178, New Programs Should Meet DO-178B Objectives
- This Notice Explains How to Make the Transition from DO-178/178A Without Re-engineering all of the Data

107

Topic 5
NB110.78

Equivalence of SW Levels (Section 5a)

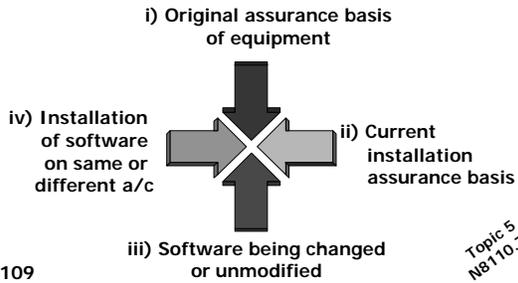
- Software Level Must Be Shown to be Equivalent or Better; Otherwise, Use 12.1.4

Table 1
Software Level Equivalence

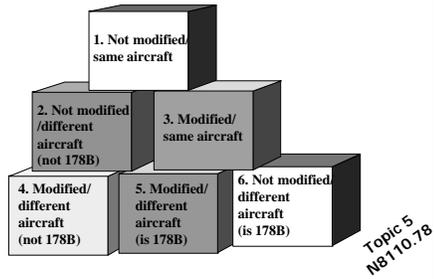
DO-178B SW Level Required by the Installation	Legacy System Software Level per DO-178/DO-178A		
	Critical/Level 1	Essential/Level 2	Non-essential/Level 3
A	YES/Analyze	NO	NO
B	YES	NO/Analyze	NO
C	YES	YES	NO
D	YES	YES	NO
E	YES	YES	YES

108

4 Variables (Section 5b)



Six Categories (Section 5b)



Applicability (Section 5c)



- Notice Not Directly Applicable to TSOs
- May be Applied to TSOs, at Discretion of the ACO

111

Topic 5
Ns110.78

Small, Simple Change (Section 5d)

1/2



- Small, Simple Change--
New Terminology
- Intended to Address the
"Very Minor" Changes That
Have Little or No Effect on
Installation
- System to Be Used the
Same
- Shouldn't Apply if Service
Difficulties Exist
- Must Be Agreed Upon With
the ACO Engineer

112

Topic 5
NB110.78

Small, Simple Change (Section 5d)

2/2

- Once Agreed Upon, Treated as
Systems Under the Original Approval
Basis
 - I.e., Like Pre-178B Changes
- Examples: Change to Already Tested
Gain Setting, Maintenance Data , ...

113

Topic 5
NB110.78

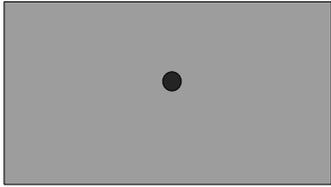
**Handling Changes With 178B As
Part of Cert Basis (Section 5e) - 1/4**

- If It's Not a Small, Simple Change:
 - Use DO-178B to Evaluate:
 - Processes Used to Make the Change
 - Changed Components
 - Components Affected by the Change
 - Unaffected Portions Require No
Further Analysis

114

Topic 5
NB110.78

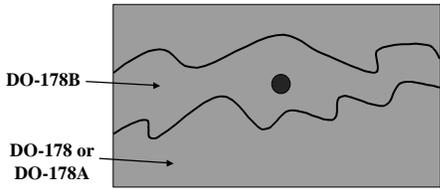
**Handling Changes With 178B As
Part of Cert Basis (Section 5e) - 2/4**



115

Topic 5
NB110.78

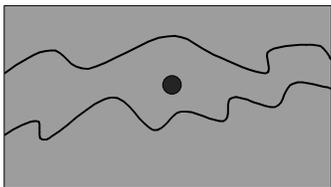
**Handling Changes With 178B As
Part of Cert Basis (Section 5e) - 3/4**



116

Topic 5
NB110.78

**Handling Changes With 178B As
Part of Cert Basis (Section 5e) - 4/4**



117

Topic 5
NB110.78

Equivalency (Section 6a)

- Start With Equivalency Determination
- If Equivalency Not Established, Use 178B 12.1.4

Table 1
Software Level Equivalence

DO-178B SW Level Required by the Installation	Legacy System Software Level per DO-178/DO-178A		
	Critical/Level 1	Essential/Level 2	Non-essential/Level 3
A	YES/Analyze	NO	NO
B	YES	NO/Analyze	NO
C	YES	YES	NO
D	YES	YES	NO
E	YES	YES	YES

118

Six Categories (Section 6b-e)

- Evaluate project based on 6 categories (5b):** Section 6
Correlation
1. Not modified/same aircraft
 2. Not modified/different aircraft (not 178B) → Section 6b
 3. Modified/same aircraft
 4. Modified/different aircraft (not 178B) >→ Section 6c
 5. Modified/different aircraft (is 178B) →→ Section 6d
 6. Not modified/different aircraft (is 178B) →→ Section 6e

119 Correlation Between Section 5b and 6b-e

An Example (Section 6b-e)

- Assume A TCAS II Unit Is To Be Evaluated for Multiple Installations
- The Original TCAS II Unit Was Developed Using DO-178A, Level 2
- Assume the Original TCAS II Unit Was Installed on a Citation V, That Required DO-178A

120

Topic 5
NB110.78

**SW Not Modified/
Same or Different Non-178B Aircraft
(Section 6b)**

- **Example:** Original TCAS II Unit Installed on Citation V Upgrade or Citation II Aircraft (Both Aircraft Are Non-178B)
- Accept Original Assurance Process (I.e., Use Pre-178B Process)
- Applies Only if System is Used Exactly the Same As In Original Cert
- Applies Only if System Has Not Experienced Service Difficulties

121

Topic 5
NB110.78

**SW Modified/
Same or Different Non-178B Aircraft
(Section 6c)**

- **Example:** Assume TCAS II Unit Modified To Add a Special Pop-up Feature and Will Be Re-installed on Both the Citation V and Its Upgrade
- Assess If TCAS II Unit Is Used In The Same Manner
- Use Original Assurance Method of Aircraft or System (I.e., Use Pre-178B Process)

122

Topic 5
NB110.78

**SW Modified/
Different Aircraft Requiring 178B
(Section 6d) 1/2**

- **Example:** Assume TCAS II Unit is Modified to Add a Special Pop-up Feature and will be Installed on a Citation XXX (With 178B As Part of the Cert Basis)
- Assess if the Change is a Small, Simple Change

123

Topic 5
NB110.78

**SW Modified/
Different Aircraft Requiring 178B**
(Section 6d) 2/2

- **If Small, Simple Change:**
 - Handle Change As If DO-178B Didn't Exist (I.e., Follow the Already Established 178A Process)
- **If Not Small, Simple Change:**
 - Make Changes Using DO-178B as Described in Section 5e

124

Topic 5
NB110.78

**SW Not Modified/
Different Aircraft Requiring 178B**
(Section 6e)

- **Example:** Assume Original TCAS II Unit Installed on a Citation XXX (With 178B As Part of the Cert Basis)
- Original Approval May Be Accepted, If There are No Significant Operational Differences
- Significance of Operational Changes is at Discretion of ACO or Delegated DER

125

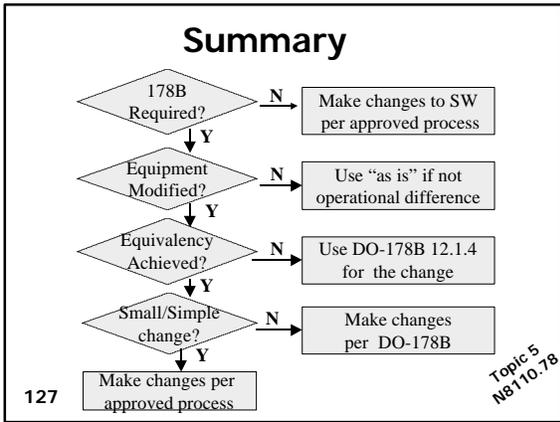
Topic 5
NB110.78

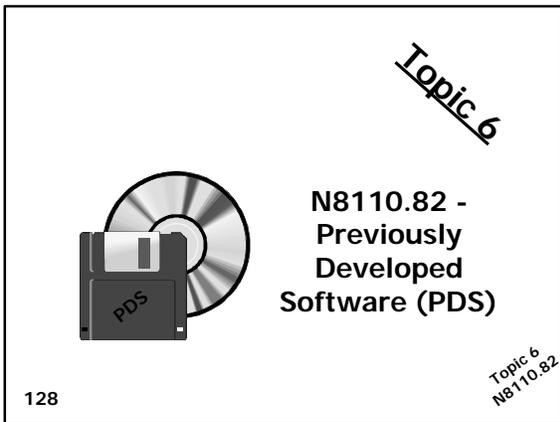
**Documentation & Further
Changes** (Section 6f and 6g)

- Changes To Legacy Systems And Their Processes, Should Be Documented in PSAC, CID, and/or SAS
- Any Further Changes to the System? Use the Notice Again

126

Topic 5
NB110.78





Purpose & History

- **PURPOSE:**
 - To Give Guidelines For Meeting DO-178B Level D Objectives For PDS
- **HISTORY:**
 - Began When Applicant Desired To Use Windows NT On Their Airborne Equipment
 - PDS Is Big Issue For Industry
 - Routed For Comment Sept 1998
 - Signed March 1999

129 Topic 6
N8110.82

Technical Information: What Is PDS?

- Software that was not developed using DO-178B
 - Commercial-off-the-shelf
 - Military Standards
 - Other Industry Standards
 - DO-178 or DO-178A
 - etc.



130



Tech Info: Consider

- If autos advanced as fast as computers:
 - V-32 instead of a V8
 - Top speed of 10,000 miles per hour
 - Get thousands of miles to the gallon
 - Of course the cost would be \$49.95 ...but
- Do you really want a car that crashes twice a day?

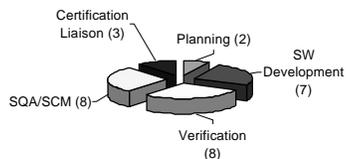


131



Technical Info: Level D Objectives - 1/7

28 Level D Objectives



Topic 6
NR170.82

132

**Technical Info: Level D
Objectives - 2/7**

- Two Planning Objectives: 1-1, 1-4
- There Must Be a Plan (per 1-1)
 - Don't Evaluate Quality of Plan (1-6)
 - Plan May Not Meet DO-178B (1-6)
- Plan Must Be Followed
- Additional Considerations Should Be In The Plan (1-4)
 - Magic
 - Service Experience

133

Topic 6
NB110.82

**Technical Info: Level D
Objectives - 3/7**

- Eight SQA/SCM Objectives
 - Plan Was Carried Out
 - Product Configuration Is Identified, Protected, And Explained
 - What Is Approved Is What Is Flying

134

Topic 6
NB110.82

**Technical Info: Level D
Objectives - 4/7**

- Three Certification Liaison Objectives:
 - Cert Authority Agreement Up Front
 - Data In Place To Prove:
 - Plan Was Followed
 - DO-178B Objectives Were Met

135

Topic 6
NB110.82

**Technical Info: Level D
Objectives - 5/7**

- **Eight Verification Objectives**
 - Six Concentrate on Functional Testing
 - High Level Req Good & Trace to Sys Req
 - Executable Complies and Is Robust With High Level Req
 - One Verifies Behavior of Object Code in Target Environment
 - Executable Code Compatible w/ Target Computer
 - One Verifies That Partitioning Is Not Compromised

Topic 6
NB110.82

136

**Technical Info: Level D
Objectives - 6/7**

- **Seven Development Objectives: Table A-2**
 - 2-1: High Level Req Developed
 - 2-2: Derived High Level Req Are Defined
 - 2-3, 2-4, 2-5: SW Architecture/Low Level Req Are Developed
 - ... From High Level Req
 - No Verification Objectives Cover This

Topic 6
NB110.82

137

**Technical Info: Level D
Objectives - 7/7**

- **Seven Development Objectives (cont)**
 - 2-6: Source Code Is Developed
 - ... Traceable to and Conforms with Low Level Req
 - No Verification Objectives Cover This
 - 2-7: Object Code is Produced and Executes in Target Computer
 - No Verification Objectives Cover This
 - High Level Req Testing Subsumes This

Topic 6
NB110.82

138

Notice Outline

- **7 Sections:**
 - Section 1: Purpose
 - Section 2: Distribution
 - Section 3: Related Publications
 - **Section 4:** Background
 - **Section 5:** Discussion
 - **Section 6:** Procedures
 - Section 7: Conclusion

139

Topic 6
NB110.82

Background (Section 4) - 1/2

- Level D to Address a Minor Aircraft Failure Condition
- Level D Intended to Provide a Thorough Investigation of the Functional Behavior of the Software
- Level D Intended to Provide the Necessary Configuration Control

140

Topic 6
NB110.82

Background (Section 4) - 2/2

**28
Objectives**

141

Topic 6
NB110.82

Discussion (Section 5)



5 Confusing Objectives
1-1, 2-3, 2-4, 2-5, 2-6

Topic 6
NB110.82

142



Objective 1-1 (Section 5a)

- 1-1, "Software Development and Integral Processes Activities are Defined," Req'd for Level D
- 1-6, "Software Plans comply with this document," Not Req'd For Level D
- Interpretation:
 - There Must Be Plans (1-1)
 - Plans Should Assure SW Meets DO-178B Objectives
 - Plans Must Be Followed (9-1)

Topic 6
NB110.82

143

Objective 2-4 (Section 5b)

- 2-4: "Low-level Requirements Are Developed"
- Intent: Design Is Defined
- No Explicit Verification of Low Level Req or Architecture In Table A-4
- 2-4 Is Implicitly Satisfied By 6-1 & 6-2
- No Need To Assure Low Level to High Level Req Traceability for Level D PDS

Topic 6
NB110.82

144

Objective 2-3 (Section 5c)

- 2-3: "Software Architecture Is Developed"
- Same Logic As Objective 2-4
- No Explicit Verification Activities
- Implicitly Satisfied By Other Objectives
 - I.e., 4-8 through 4-12

145

Topic 6
NB110.82

Objective 2-5 (Section 5d)

- 2-5: "Derived Low-Level Requirements Are Defined"
- No Explicit Verification of Derived Low-Level Requirements
- Implicitly Satisfied By Meeting Objective 2-2 and Associated Verification of High Level Requirements

146

Topic 6
NB110.82

Objective 2-6 (Section 5e)

- 2-6: "Source Code Is Developed"
- No Explicit Verification of Source Code In Table A-5
- Need: Exe Code to High Level Req Traceability
- Don't Need: Source Code to Low-Level Req to High-Level Req Traceability
- Interpretation: Exe Code to Meet All Functional Verification Requirements By Other Objectives

147

Topic 6
NB110.82

Procedures (Section 6)

- a) Table A-2, objectives 3,4,5,6 are Implicitly Covered by Other Objectives
- b) Partitioning/Protection for Systems with Multiple Function
- c) May Need to Limit Software Level for PDS in Systems with Multiple Functions

148

Topic 6
NB110.82

Example - 1/4

- A Company Recently Received A TSO Approval On A System Using Windows NT
- The System Was A Level C Moving Map/ Navigation Device
- However, Windows NT Was Only Approved To Level D
- Required Protection Between System (Level C) And Windows NT (Level D)
- Windows NT Was Shown To Provide Only a Minor Failure Condition

149

Topic 6
NB110.82

Example - 2/4

- Protection Argument Required Applicant To Demonstrate:
 - No Failure of Windows NT Can Contribute to Anything Greater Than a Minor Hazard
- OR
- No Failure of NT Can Affect Other Programs

150

Topic 6
NB110.82

Example - 3/4

- **Three Choices For Windows NT Approval To Level D**
 - Meet Objectives for Level D
 - Sublimate as Part of Architecture
 - Service Experience

151

Topic 6
NB110.82

Example - 4/4

- **SUMMARY OF EXAMPLE:**
 - Moving Map/Navigation Device - Can Produce a Major Hazard
 - Windows NT Was Shown to Produce Only a Minor Failure Condition
 - By Considering Loss of Function vs Corruption of Function
 - By Converting all Windows NT Problems to Loss of Function

152 – Windows NT is NOT Level C

Topic 6
NB110.82

SC-190/WG-52's Activities

- **SC-190/WG-52 Addressing PDS**
 - Started As: "COTS" Sub-group
 - Became: "PDS" Sub-group
 - Now: "Development" Sub-group
- **Writing Frequently Asked Questions (FAQs) and Position Papers To Clarify DO-178B**

153

Topic 6
NB110.82

COTS Research Project

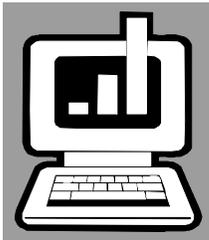
- AIR-130 Sponsoring a Research Project On COTS Hardware and Software
- Goals: Develop Criteria And Tutorial For COTS Use In Aviation Systems



Topic 6
N8110.82

154

Topic 7



Tool Qualification N8110.83

Topic 7
N8110.83

155

Purpose & History - 1/2

- Purpose:
 - Provide Guidelines To ACO Engineers and DERs For Software Tool Qualification
 - Clarify Difference Between Development and Verification Tools
 - Clarify DO-178B Guidance On Tools Qualification

Topic 7
N8110.83

156

Purpose & History - 2/2

• History:

- Identified At Streamlining Software Aspects Of Certification (SSAC) Workshop #1 (Jan 1998) As Confusing Part of DO-178B
- SSAC Workshop #2 (May 1998) - Began Work On Position
- Draft Notice Routed For Comments - Sept 98
- Notice Completed - April 1999

157

Topic 7
Ns110.83

Technical Info: What is A Tool? 1/3



• Dictionary

- A Means To An End
- Anything Used in Performing an Operation
- Anything Regarded as Necessary to the Carrying Out of One's Occupation or Profession

• Leanna's Definition

- Something That Helps Get The Job Done By Reducing the Time and Effort Required

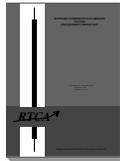
158

Topic 7
Ns110.83

Technical Info: What is A Tool? 2/3

• DO-178B Definition a Software Tool:

- A computer program used to develop, test, analyze, produce, or modify another program or its documentation.



159

Technical Info: What is A Tool? 3/3

- DO-178B Defines Two Software Tools:
 - Software Development Tools: “Tools whose output is part of airborne software and thus can introduce errors.”
 - Tool that can inject an error into the software.
 - Software Verification Tools: “Tools that cannot introduce errors, but may fail to detect them.”
 - Tool that may not detect an error with the software.

160

Topic 7
N8110.83

Technical Info: Examples

Development	Verification
<ul style="list-style-type: none"> • autocode generators • compilers • software libraries • operating systems 	<ul style="list-style-type: none"> • simulators • emulators • test tools - coverage analyzers • test case generators

161

Topic 7
N8110.83

Technical Info: So .. What's Tool Qualification?

- Process To Ensure That A Tool Provides Confidence At Least Equivalent To The Processes That Are Eliminated, Reduced, or Automated
- See DO-178B, Section 12.2
- Alternative: Verification of Tools Outputs per DO-178B Section 6
- Notice N8110.83 Provides Guidelines

162

Topic 7
N8110.83

Notice Outline

- **7 Sections:**
 - Section 1: Purpose
 - Section 2: Distribution
 - Section 3: Related Publications
 - Section 4: Background
 - Section 5: Discussion
 - Section 6: Procedures
 - Section 7: Conclusion

163

Topic 7
NB110.83

Background (Section 4) - 1/3

- Tools Are Developed to Eliminate, Reduce, or Automate Portions of the Process
- Obtain Confidence by Qualification
- DO-178B, Section 12.2 Addresses Tool Qualification
- Section 12.2 → → 8 Areas of Confusion

164

Topic 7
NB110.83

Background (Section 4) - 2/3



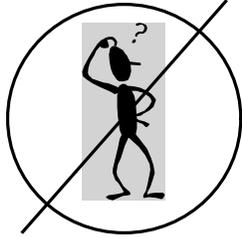
8 Areas of Confusion

165

1. When to Qualify A Tool
2. Different Types of Criteria
3. Applicable Criteria for Tool Qualification
4. Data Production for Tool Qualification
5. Tool Operational Requirements Acceptance Criteria
6. Tool Determinism
7. Tool Partitioning Assurance
8. Tool Configuration Control

Topic 7
NB110.83

Background (Section 4) - 3/3



166 Notice Intended to Abolish Confusion

Topic 7
NS110.83

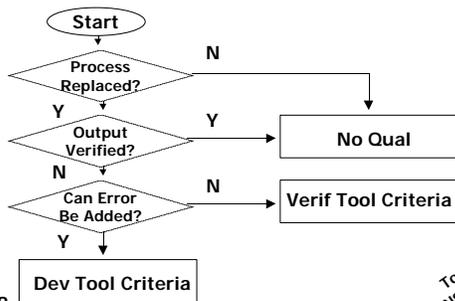
When Is Tool Qualification Needed? (Section 5 - Discussion) - 1/2

- DO-178B, 12.2 Tool Qualification states, "Qualification of a tool is needed when processes of this document are eliminated, reduced or automated by the use of a software tool without its output being verified as specified in section 6."



167

When Is Tool Qualification Needed? (Section 5) - 2/2

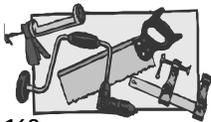


168

Topic 7
NS110.83

Two Types of Tools (Section 5)

1. Verification



2. Development

169

Topic 7
Ns110.83

Verification Tools (Section 5) - 1/2

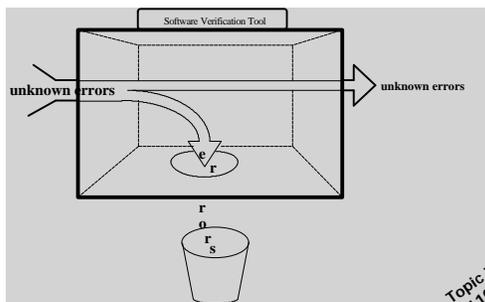
- Tools that cannot introduce errors, but may **fail to detect** them.
 - For example, a static analyzer, that automates a software verification process activity, should be qualified **if the function** that it performs is **not verified** by another activity. Type checkers, analysis tools and test tools are other examples.



170

Topic 7
Ns110.83

Verification Tools (Section 5) - 2/2



171

Topic 7
Ns110.83

Development Tools

(Section 5) - 1/2

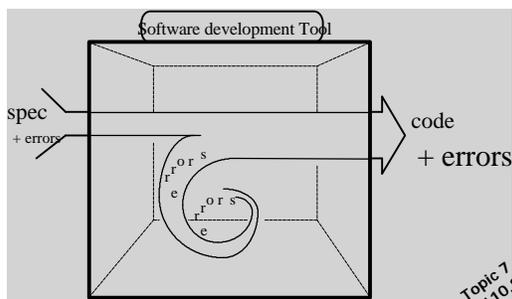
- Tools whose output is part of airborne software and thus can introduce errors.
- For example, a tool which generates Source Code directly from low-level requirements would have to be qualified if the generated Source Code is not verified as specified in section 6.



172

Topic 7
Ns110.83

Development Tools (Section 5) - 2/2

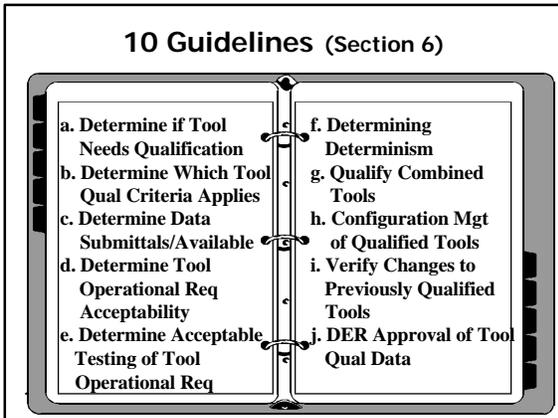


173

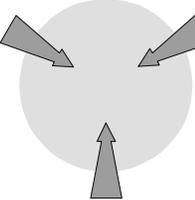
Topic 7
Ns110.83

10 Guidelines (Section 6)

- Determine if Tool Needs Qualification
- Determine Which Tool Qual Criteria Applies
- Determine Data Submittals/Available
- Determine Tool Operational Req Acceptability
- Determine Acceptable Testing of Tool Operational Req
- Determining Determinism
- Qualify Combined Tools
- Configuration Mgt of Qualified Tools
- Verify Changes to Previously Qualified Tools
- DER Approval of Tool Qual Data



Three Questions To Determine If Tool Qual Is Needed (Section 6a) - 1/3

- 
- 1. Can tool insert error or allow an existing error to remain undetected?
 - 2. Will tool's output not be verified per section 6 of DO-178B?
 - 3. Are processes required by DO-178B objectives eliminated, reduced, or automated?

175

Topic 7
NB110.83

Three Questions To Determine If Tool Qual Is Needed (Section 6a) - 2/3

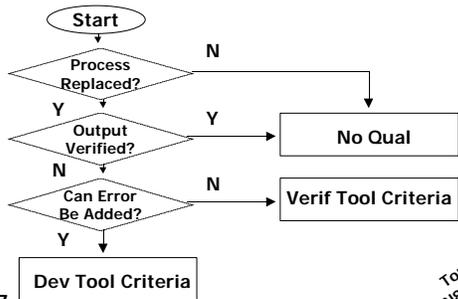


• **QUALIFY:** If All 3 Questions Are Answered YES.

176

Topic 7
NB110.83

Three Questions To Determine If Tool Qual Is Needed (Section 6a) - 3/3



177

Topic 7
NB110.83

Documenting (Section 6a)

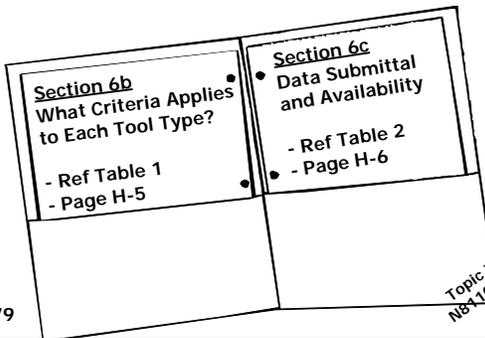


- All Tools Should Be Documented in the Plan for Software Aspects of Certification (PSAC)

178

Topic 7
Ns110.83

Sections 6b and 6c



179

Topic 7
Ns110.83

Data Submittals (Section 6c)

- | | |
|--|---|
| <ul style="list-style-type: none">• Development tool• Plan for Software Aspects of Certification• Tool Qualification Plan• Tool Operational Requirement• Tool Accomplishments Summary• Software Accomplishment Summary | <ul style="list-style-type: none">• Verification tool• Plan for Software Aspects of Certification• Tool Operational Requirements• Software Accomplishment Summary |
|--|---|

180

Topic 7
Ns110.83

Tool Operational Requirement (Section 6d)

- **Development tool**
 - Functionality
 - Operational Environment
 - Installation or Operational Info
 - Development Process Performed
 - Expected Response Under Abnormal Conditions
- **Verification tool**
 - Functionality
 - Operational Environment
 - Installation or Operational Info

181 Topic 7
NB110.83

Tool Operational Requirement (Section 6e)

- **Verification Tools**
 - Normal Operating Conditions
 - Only Test Used Portion
- **Development Tools**
 - Normal Operating Conditions
 - Abnormal Operating Conditions
- See DO-178B Section 6.4.2 For "Normal" vs. "Abnormal"

182 Topic 7
NB110.83

Determinism of Tools
(Section 6f)

- **Ability to Establish Correctness of the Output from the Tool**
- **Given the Same Input, the Tool Should Generate the Correct Output Every Time**
 - All Possible Variations of the Output from Some Given Input Should Be Correct
 - Variations in Output Need to be Bounded; e.g., Case/Switch Construct in a Code Generator

183 Topic 7
NB110.83

Combined Tools (Section 6g)

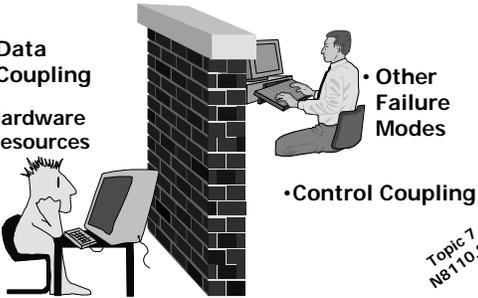
- Output of Both are Used to Meet or Replace DO-178B Objectives
- May Be Qualified Separately When Protection/Partitioning Between Tools is Shown

184

Topic 7
NB110.83

Examples of Protection/Partitioning (Section 6g)

- Data Coupling
- Hardware Resources
- Control Coupling
- Other Failure Modes



185

Topic 7
NB110.83

Configuration Management (Section 6h)

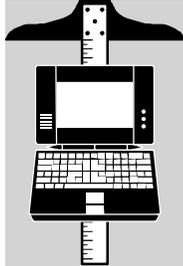
- Configuration Management Must Be Applied for Credit
 - DO-178B, 12.2.3b and 7.3.9b
 - Tools, if Used for Credit, Generally Handled as CC2, Although Some CC2 Prescriptions May Not Apply to Tools Purchased Commercially (e.g., Traceability and Change Control)

186

Topic 7
NB110.83

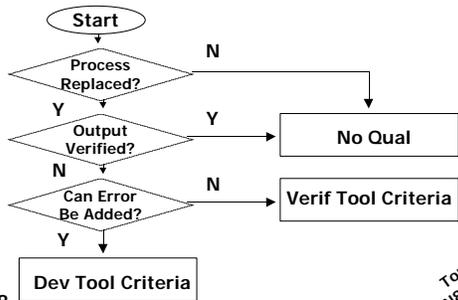
Section 6i and 6j

- 6i: Changes to Qualified Tools
 - Change Impact Analysis
- 6j: DERs
 - Don't Delegate if Alternate Means or Policy Issues Exist



187

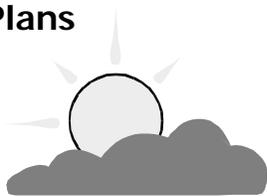
Summary



188

Topic 7
Ns110.83

Future Software Policy & Guidance Plans



Topic 8

Topic 8
Future

189

Policy Currently In Work

- Major/Minor Software Changes
- Reuse of Software Life Cycle Data
- Roles and Responsibilities for Software Personnel
- Level of FAA Involvement Criteria For Software Projects
- ACSEP Order With Improved Software Criteria

190

Topic 8
Future

Future Policy/Guidance Being Planned

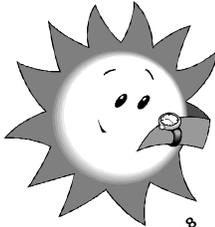
- Software Conformity Policy
- Production Software Guidance (Dr. Singh)
- Software Reuse (3rd Party Software)
- Software Order (Combine Notices)

191

Topic 8
Future

New Issues?

- New Issues Constantly Arising
- Contact AIR-130 If You Know of Software Policy Issues
- Examples: Auto-code Generators, Reusable Software, Object-Oriented Technologies, Run-Time Libraries, Cyclic Redundancy Checks, etc.



192

Topic 8
Future

RTCA/EUROCAE Activities

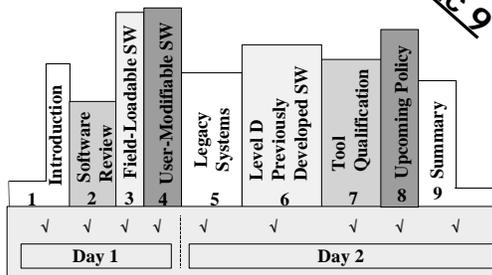
- SC-190/WG-52
 - Errata
 - Frequently Asked Questions
 - Discussion Papers
 - ANNUAL REPORT
- SC-182
 - Avionics Computer Resource
 - MOPS/TSO

193

Topic 8
Future

Summary

Topic 9



194

Software Policy Bookshelf

NOTES:

N8110.81 – Software Review Process Notice

Appendix B

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.81

3/19/99

Cancellation
Date: 3/19/00

SUBJ: GUIDELINES FOR THE SOFTWARE REVIEW PROCESS

1. PURPOSE. This notice provides guidelines to Aircraft Certification Service (AIR) field offices (i.e., Aircraft Certification Offices and Manufacturing Inspection District or Satellite Offices) and to Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," for conducting software reviews. Advisory Circular (AC) 20-115B, "RTCA, Inc. Document RTCA/DO-178B," recognizes DO-178B as an acceptable means of compliance for securing the Federal Aviation Administration's (FAA) approval of software in airborne systems and equipment. This notice establishes guidelines for conducting software reviews during the software development life cycle of airborne systems and equipment that are developed to meet the objectives of DO-178B.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

c. FAA Job Aid, "Conducting Software Reviews Prior to Certification," dated June, 1998.

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL),
A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220
(25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

4. DEFINITIONS. For the purpose of this notice, the following definitions apply:

a. Review is the act of inspecting or examining software life cycle data, software project progress and records, and other evidence made with the intent of finding compliance with DO-178B objectives. Review is an encompassing term and may consist of a combination of reading, interviewing project personnel, witnessing activities, sampling data, and participating in presentations. A review may be conducted at one's own desk, at an applicant's facility, or at an applicant's supplier's facility.

b. Sampling is the process of selecting a representative set of software life cycle data for inspection or analysis to attempt to determine the compliance of all the software life cycle data developed up to that point in time in the project. Sampling is the primary means of assessing the compliance of the software processes and data. Examples of sampling may include any or all of the following:

(1) An inspection of the traceability from system requirements to software requirements to software design to source code to object code to test cases and procedures to test results.

(2) A review of any analyses used to determine system safety classification and software level, or of any reviews or analyses used to meet any DO-178B objective (e.g., timing analysis or code review).

(3) An examination of the structural coverage of multiple samples of source code modules.

(4) An examination of multiple samples of software quality assurance records and configuration management records.

c. Presentation is useful for providing emphasis on important issues or solutions or for clarifying points of question before the largest possible audience at the same time. Presentations should be used sparingly in assessing software, as the presentation data is general in nature and tends to provide an idealized and static abstraction of the actual processes. In obtaining review results of software life cycle processes, the productivity of presentations is typically low. Presentations combined with sampling is more effective. Presentations generally provide an overview of what was supposed to transpire during the development activities. Sampling provides a view of what actually transpired. Inconsistencies between presentation information and sampling data can provide certification authorities and designees insight into the actual life cycle activities. Inconsistencies can also provide management with important feedback data for continuous improvement.

d. Finding is the identification of a failure to show compliance to one or more of the DO-178B objectives.

e. Observation is the identification of a potential software life cycle process improvement.

5. SCOPE.

a. Section 9 of DO-178B describes the certification liaison process. The certification liaison process is the vehicle to establish communication and understanding between the applicant and the certification authority. Sections 9.2 and 10.3 of DO-178B state that the certification authority may review the software life cycle processes and data to assess compliance to DO-178B. This notice does not change the intent of DO-178B with regard to the software review process but clarifies the application of DO-178B.

b. Although desk reviews may be used to successfully accomplish the software review process, this notice primarily focuses on on-site reviews. The desk review uses similar techniques as the on-site review but does not have the advantages of being on-site (e.g., access to software personnel, access to all automation, access to test set-up). Both on-site and desk reviews may be delegated to properly authorized designees. Practical arrangements with the software developer for FAA on-site reviews should include:

- (1) Agreement on the type of review(s) that will be conducted (i.e., planning, development, verification, or final certification).
- (2) Agreement on date(s) and location(s) of the review(s).
- (3) Identification of the certification authority's personnel involved.
- (4) Identification of any designees involved.
- (5) Development of the agenda(s) and expectations.
- (6) Listing of software data to be made available (both prior to the review(s) and at the review(s)).
- (7) Clarification of procedures intended to be used.
- (8) Identification of any required resources.
- (9) Specification of date(s) and means for communicating review results (may include corrective actions and other required post-review activities).

c. The objectives of the software review process are found in Section 6 of this notice. Section 7 of this notice primarily addresses the integration of the software review process with the software development life cycle. Section 7 also identifies the four types of reviews and the software life cycle data and data assessment criteria for each type. Section 8 of this notice addresses additional considerations for the software review process. Section 9 of this notice provides guidelines for preparing, conducting, and documenting the software review.

6. OBJECTIVES OF THE SOFTWARE REVIEW PROCESS.

a. The certification authority may review the software life cycle processes and associated data at his or her own discretion to obtain assurance that a software product submitted as part of a certification application complies with the certification basis and the objectives of DO-178B. The software review process assists both the certification authority and the applicant in determining if a particular project will meet the certification basis and DO-178B objectives by providing:

(1) Timely technical interpretation of certification basis and DO-178B objectives, FAA policy, issue papers, and other applicable certification requirements.

(2) Visibility into the implementation compliance and the applicable data.

(3) Objective evidence that the software project adheres to its approved software plans and procedures.

(4) The opportunity for the certification authority to monitor designee activities.

b. The amount of FAA involvement in a software project should be determined and documented as soon as possible in the project life cycle. The type and number of software reviews will depend on the software level of the project, the amount and quality of designee support, the experience and history of the applicant and/or software developer, service difficulty history, and several other factors. The specifics for determining and documenting the level of FAA involvement in software projects will be addressed in future FAA policy.

7. INTERACTION BETWEEN THE SOFTWARE REVIEW PROCESS AND SOFTWARE LIFE CYCLE.

a. The review process should begin early in the software life cycle. The early involvement will mitigate the risk that the system, software, and planning decisions will not comply with the DO-178B objectives. This requires timely communication between the applicant and ACO engineer regarding those planning decisions that may impact the software product and processes. Typically, the development of software associated with an aircraft or engine component or a Technical Standard Order (TSO) appliance may take several months or years. Since DO-178B is process-orientated guidance, to be meaningful the review process should be integrated throughout the software life cycle. This means that regular contact between the applicant and FAA should be established. This contact should provide gradually increasing confidence in the software life cycle processes and the resultant product to both the applicant and the FAA. The four types of reviews are described as follows:

(1) A software planning review should be conducted when the initial software planning process is complete (i.e., when most of the plans and standards are completed and reviewed).

(2) A software development review should be conducted when most of the software development data (i.e., requirements, design, and code) are complete and reviewed.

(3) A software verification review should be conducted when most of the software verification and testing data are complete and reviewed.

(4) A final certification software review should be conducted after the final software build is completed, the software verification is completed, a (preliminary) software conformity review has been conducted, and the software product is ready for formal system certification approval.

b. Availability of software life cycle data does not imply that the data is always complete. However, the data should be sufficiently mature so that a reasonable review can be conducted. Similarly, all transition criteria may not necessarily be complete for that time in the project, but sufficient transition criteria evidence should exist to ensure they are being applied to the project.

c. Discussions between the applicant and the FAA occurs early in the project life cycle and should determine the types, need, number, depth, and format of the software reviews. For the purpose of this notice, four reviews are identified to assess compliance to DO-178B objectives. As previously stated, the level of FAA involvement in the software project will be further documented in future policy.

d. The following paragraphs define the basic goals of each of the four types of software reviews, the criteria for each type of review (e.g., type and availability of data, type of transition criteria), and the appropriate evaluation criteria. Section 8 of this notice identifies additional considerations that may impact the type and timing of reviews.

(1) Software Planning Review

(a) Identification of the Software Planning Review. The software planning process is the initial process in the software life cycle for any software project. The planning process establishes the various software plans, standards, procedures, activities, methods, and tools required to develop, verify, control, assure, and produce the software life cycle data. The intent of the software planning review is to determine if the applicant's plans and standards provide an acceptable means for complying with the objectives of DO-178B. This review can also reduce the risk of an applicant producing a software product inconsistent with the certification criteria and which will not support the continued airworthiness requirements of the product. The software planning review should take place after the initial completion of the software planning process. Although the software planning process may continue throughout the software life cycle, and plans and standards may change as the project progresses, it is generally considered complete when the associated initial transition criteria are satisfied. The following transition criteria are indicative of typical software planning process completion criteria:

1. Software plans and standards have been internally reviewed based on company specified criteria and deficiencies resolved.

2. Software plans and standards have been evaluated by software quality assurance and deficiencies resolved.

3. Software plans and standards have been approved and placed under configuration control.

4. The objectives of DO-178B, Annex A, Table A-1 have been satisfied.

(b) Data Required for the Software Planning Review. The applicant should make the software plans and standards shown in Table 1 available to the certification authority or designee (if appropriate). The supporting software data should be under configuration control, appropriate for the software level, prior to the software planning review.

Software Data	DO-178B Section
Plan for Software Aspects of Certification	11.1
Software Development Plan	11.2
Software Verification Plan	11.3
Software Configuration Management Plan	11.4
Software Quality Assurance Plan	11.5
*Software Requirements, Design, and Code Standards	11.6, 11.7, 11.8
Tool Qualification Plans, if applicable	12.2, 12.2.3.1
Software Quality Assurance Records as applied to the planning activities	4.6, 11.19

* Not required for Level D, per DO-178B, Annex A, Table A-1.

Table 1. Data Availability for Software Planning Review

(c) Evaluation Criteria for the Software Planning Review. The objectives which apply to planning in DO-178B Annex A, Tables A-1 (all objectives), A-8 (objectives 1-4), A-9 (objective 1), and A-10 (objectives 1-2), should be used as the evaluation criteria for the software planning review. Additionally, the applicant’s safety assessment, failure conditions, and software level(s) should be assessed. The relevance of the software plans and standards to the software level should also be evaluated.

(2) Software Development Review

(a) Identification of the Software Development Review. The software development processes are the software requirements, design, code, and integration processes. The development processes are supported by the integral processes of software verification, configuration management, quality assurance, and certification liaison processes. Therefore, the software development review should assess the effective implementation of the applicant's plans and standards through examination of the software life cycle data, particularly the

software development data and integral processes' data associated with it. During this review, the applicant and FAA may come to agreement on changes to or deviations from plans and standards that are discovered during the review. Before conducting a software development review, the software development data should be sufficiently complete and mature to ensure that enough evidence exists that the developer is complying with their approved plans, standards, and transition criteria. The following are typical criteria for a sufficiently mature software development process:

1. High-level requirements are documented, reviewed, and traceable to system requirements.
2. Software architecture is defined, and reviews and analyses have been completed.
3. Low-level requirements are documented, reviewed, and traceable to high-level requirements.
4. Source code implements and is traceable to the low-level requirements and has been reviewed.

(b) Data Required for the Software Development Review. For a software development review, the software data shown in Table 2 should be made available to the certification authority. The supporting software data should be under configuration control, as appropriate for the software level, prior to the review.

Software Data	DO-178B Section
*Software Requirements, Design and Code Standards	11.6, 11.7, 11.8
Software Requirements Data	11.9
Design Description	11.10
Source Code	11.11
Software Verification Results (as applied to DO-178B, Annex A, Tables A-2 through A-5)	6.3.1, 6.3.2, 6.3.3, 6.3.4, 11.14
Software Life Cycle Environment Configuration Index	11.15
Problem Reports	11.17
Software Configuration Management Records	11.18
Software Quality Assurance Records (as applied to DO-178B, Annex A, Tables A-2 through A-6)	11.19

* Not required for Level D, per DO-178B, Annex A, Table A-1.

Table 2. Data Availability for the Software Development Review

(c) Evaluation Criteria for the Software Development Review. The objectives which apply to development in DO-178B, Annex A, Tables A-2 (objectives 1-6), A-3 (all objectives), A-4 (all objectives), A-5 (objectives 1-6), A-8 (objectives 1-4, 6), A-9 (objectives 1-2), and A-10 (objective 3), should be used as evaluation criteria for this review. Additionally, the software life cycle data should be evaluated to determine the effectiveness of the applicant's plans and standards implementation in the development process.

(3) Software Verification Review

(a) Identification of Software Verification Review. The software verification process is typically a combination of inspections, demonstrations, reviews, analyses, tests, and test coverage analysis. As with the other reviews, the software configuration management and quality assurance processes are also active during these verification activities. The verification activities confirm that the software product specified is the software product built. Therefore, the software verification review should ensure that the software verification processes will provide this confirmation and will result in objective evidence that the product has been sufficiently tested and is the intended product. The purpose of the software verification review is to: assess the effectivity and implementation of the applicant's verification plans and procedures; ensure the completion of all associated software configuration management and quality assurance tasks; ensure that the software requirements and design have been verified; and ensure that the software verification process will achieve the structural coverage criteria of DO-178B, Annex A, Table A-7. Before conducting a software verification review, the software verification process should be sufficiently complete and mature to ensure that the representative verification data exists to assess that the applicant's approved plans and standards are being complied with and evidence exists that transition criteria have been met. The following criteria are indicative of a mature verification process:

1. All development data (e.g., requirements, design, source code, object code, linking and loading data, executable image) is complete, has been reviewed, and is under configuration control.
2. Test cases and procedures are documented, reviewed, and placed under configuration control.
3. Any completed testing (either formal or informal) indicates a relatively mature product.
4. Any completed testing results are documented, as agreed to in the planning documents.
5. The software testing environment is documented and controlled.

(b) Data Required for the Software Verification Review. For the purpose of compliance findings for the software verification review, the software data shown in Table 3 should be made available to the FAA. The supporting software data should be under configuration control, as appropriate for the software level, prior to the review.

Software Data	DO-178B Section
Software Requirements Data	11.9
Design Description	11.10
Source Code	11.11
Software Verification Cases and Procedures	6.3.1-6.3.6, 11.13
Software Verification Results	11.14
Software Life Cycle Environment Configuration Index (test environment)	11.15
Software Configuration Index (test baseline)	11.16
Problem Reports	11.17
Software Configuration Management Records	11.18
Software Quality Assurance Records	11.19
Software Tool Qualification Data	12.2.3

Table 3. Data Availability for Software Verification Review

(c) Evaluation Criteria for Software Verification Review. The following DO-178B, Annex A, objectives apply to the software verification review and should be used as evaluation criteria: Tables A-1 (objective 3), A-5 (objective 7), A-6 (all objectives), A-7 (all objectives), A-8 (all objectives), A-9 (objectives 1-2), and A-10 (objective 3).

(4) Final Certification Software Review

(a) Identification of Final Certification Software Review. The final software build establishes the configuration of the software product considered by the applicant to comply with all the objectives of DO-178B. It is that version of the software intended to be used in the airborne application. The purpose of this review is to: determine compliance of the final software product with the objectives of DO-178B, as defined by the software level and other software policy and guidance; ensure that all software development, verification, quality assurance, configuration management, and certification liaison activities are complete; ensure a software conformity review has been completed and the software complies; and review configuration indexes. The final certification software review should take place when the software project is completed and includes the following criteria:

1. Software conformity review has been performed and any deficiencies resolved.

2. Software Accomplishment Summary and Configuration Indexes have been completed and reviewed.

3. All software life cycle data has been completed, approved, and placed under configuration control.

(b) Data Required for Final Certification Software Review. For the purpose of this review, all software life cycle data of DO-178B should be available to FAA and/or DER. However, only the data shown in Table 4 is of special interest for this review. The supporting software data should be under configuration control, appropriate for the software level, prior to the review.

Software Data	DO-178B Section
Software Verification Results	11.14
Software Life Cycle Environment Configuration Index	11.15
Software Configuration index	11.16
Problem Reports	11.17
Software Quality Assurance Records (Software Conformity Review Report)	11.18
Software Accomplishment Summary	11.20

Table 4. Data Availability for Final Certification Software Review

(c) Evaluation Criteria for Final Certification Software Review. Evaluation criteria for this review includes all objectives of DO-178B, Annex A. Additionally, all software-related problem reports, action items, certification issues, etc. must be addressed prior to certification or authorization.

8. ADDITIONAL CONSIDERATIONS FOR THE SOFTWARE REVIEW PROCESS.

a. Although this notice proposes four types of review for FAA on-site reviews, the type, number, and extent of those reviews may not be suitable for every certification project and applicant. Additional considerations and alternative approaches may be appropriate. The following list of considerations may influence the level of the FAA involvement in the software review process:

- (1) The software level(s), as determined by a system safety assessment.
- (2) The product attributes (e.g. size, complexity, system functionality, software design).
- (3) The use of new technologies or unusual design features.
- (4) Proposals for novel software methods or life cycle model(s).

(5) The knowledge and previous success of the applicant in software development to comply with the objectives of DO-178B.

(6) The availability, experience, and authorization of software designers.

(7) The existence of issues associated with Section 12 of DO-178B in the project.

(8) The issuance of issue papers for software-specific aspects of the certification project.

b. On-site software reviews may be increased or decreased in number. Four reviews is a typical number for a Level A or Level B project; especially if no software DER is involved. Fewer or no reviews may be appropriate for some equipment manufacturers. Furthermore, reviews may be merged into a combined event or delegated to an authorized DER. It is the responsibility of the ACO engineer to determine the desired level of investigation, to plan the reviews, and to coordinate with the applicant. Criteria is being developed by the FAA to determine the appropriate level of FAA involvement in software projects. This criteria will be included in future policy.

9. PREPARING, CONDUCTING, AND DOCUMENTING THE SOFTWARE REVIEW.

This section provides guidelines for preparing for the on-site review, conducting the on-site review, and recording and communicating the review results:

a. Prepare for the On-Site Review. The responsible certification engineer should assemble the review team. The team should include at least one person knowledgeable in software engineering, one person familiar with the type of system being evaluated, and a manufacturing inspector knowledgeable in software quality assurance and configuration management (if available). The certification engineer should coordinate with the applicant regarding the upcoming software review at least six weeks in advance and propose an agenda. To optimize the efficiency of the review team while on-site, the certification authority should request the applicant to send each team member the software plans identified in DO-178B, section 4.3, several weeks prior to the review. Each team member should review the plans prior to arriving at the applicant's facility. The certification engineer should prepare a short entry briefing to introduce the team members, restate the purpose of the review, and review the agenda. The applicant should provide a short briefing to facilitate an understanding of the system under review, the software life-cycle model, processes, tools used, and any additional considerations.

Note: The specific roles and responsibilities of the FAA software review team are being documented in future FAA policy.

b. Notify the Applicant. The ACO engineer should notify the applicant in writing regarding the FAA's expectations in the software review. The following information should be included in the notification letter:

- (1) The purpose of the review and the type of review (i.e., planning, development, verification, or final).
- (2) The date and duration of the review.
- (3) A list of review participants (FAA personnel and designees) with contact information.
- (4) A request that the software plans identified in DO-178B, section 4.3, be sent to each review participant.
- (5) A request that pertinent life cycle data be made available at time of review.
- (6) An indication of which DO-178B objectives will be assessed.
- (7) A suggestion that the applicant conduct their own self-assessment prior to the review.
- (8) A request that the responsible managers, developers, verification, configuration management, and quality assurance personnel be available for questions.

c. Conduct the On-site Review. A typical on-site review includes the following elements:

- (1) Certification Authority Entry Briefing to Include: introduction of review team members; restatement of purpose of the review; and overview of the review agenda.
- (2) Software Developer's Briefing to Include: availability of facilities; availability of life cycle data; personnel schedule constraints; overview of the system; interaction of the system with other systems; system architecture; software architecture; software life cycle model (including tools and methods); progress against previous action items or issue papers (if appropriate); current status of the development; and any additional considerations (per DO-178B, section 12).
- (3) Certification Authority's Review of the Applicant/Developer's Process.
- (4) Certification Authority's Review of Product.

d. Record the Review Results. The review results should be recorded; the record should include the following, as a minimum:

(1) A list of the each life cycle data item reviewed to include: document name; control identity; version and date; requirement identification (where applicable); source code module (where applicable); paragraph number (where applicable); and review results.

(2) The approach taken to establish the finding or observation.

(3) An explanation of the findings or observations as related to the objectives of DO-178B (documented with detailed notes). Each unsatisfied objective requires a summary of what was done and a discussion as to why the objective was not satisfied. Examples should be included, when necessary. This will ensure that the approach and findings can be understood and reconstructed at some future date.

(4) Any necessary actions for either the applicant or the FAA.

(5) Listing of all current or potential issue papers.

e. Deliver an Exit Briefing. The final briefing to the manufacturer under review should be factual and positive and should summarize the findings. Findings should be presented with specific reference to DO-178B, certification basis, policy, guidance, or other certification documentation. The manufacturer should be given the opportunity to respond to the findings.

f. Identify and Prepare Issue Papers (as needed). Issue papers are a means of documenting technical and certification issues that must be resolved prior to system certification. They provide the necessary communication between applicant and certification engineer and management. Issue papers should be identified, prepared, and resolved as soon as possible after the issue is discovered. Issue papers prepared for software-specific issues should be coordinated with FAA Headquarters (AIR-130) and the appropriate Directorate.

10. CONCLUSION. The information and procedures described in this notice promote clarification and consistent application of the software review process which is part of the Certification Liaison Process described in DO-178B. This notice does not replace or supersede AC 20-115B or DO-178B.

<< Original Signed by James C. Jones >>

James C. Jones
Manager, Aircraft Engineering Division,
Aircraft Certification Service

NOTES:

N8110.77 – Field-Loadable Software Approval Notice

Appendix C

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.77

11/18/98

Cancellation

11/18/99

GUIDELINES FOR THE APPROVAL OF FIELD-LOADABLE SOFTWARE

1. PURPOSE. This notice provides guidelines to Federal Aviation Administration (FAA) Aircraft Certification Office (ACO) personnel and authorized Designated Engineering Representatives (DER) for approving field-loadable software (FLS). These guidelines are applicable to software data approvals related to type certificate (TC) approvals, amended type certificate (ATC) approvals, supplemental type certificate (STC) approvals, or Technical Standard Order (TSO) authorizations. Additional policy is being prepared to address the Parts Manufacturer Approval (PMA) process for software. This notice is for guidance purposes only and is supplemental to document RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District and Satellite Offices (MIDO and MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Title 14 Code of Federal Regulations (14 CFR) part 21, "Certification Procedures for Products and Parts."

b. Advisory Circular 21-33, "Quality Assurance of Software Used in Aircraft or Related Products."

c. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B."

d. RTCA, Incorporated, document DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. DEFINITIONS.

a. **Field-loadable software** is software that can be loaded without removal of the equipment from the installation. Field-loadable software can refer to either executable code or data. (Refer to DO-178B, paragraph 2.5.)

b. **User-modifiable software**, as the term is used in DO-178B, is software intended for modification by the aircraft operator without review by the certification authority, the airframe manufacturer, or the equipment vendor. Modifications by the user may include modifications to data, modifications to executable code, or both. (Refer to DO-178B, paragraph 2.4.)

c. **Option-selectable software** is software that contains approved and validated components and combinations of components that may be activated by the user, either through selection by the flight crew or activation by ground personnel. (Refer to DO-178B, paragraph 2.4.)

5. **BACKGROUND.** Through technological advances, the field loading of software has become a common process. This process reduces aircraft down-time for maintenance and increases efficiency of maintaining airborne equipment. DO-178B, paragraph 2.5, provides some system design considerations for FLS; however, the existing guidance for approval of FLS through the TC, ATC, STC, or TSO processes is limited. This notice provides additional guidelines for the ACO engineer or authorized DER approving FLS using the TC, ATC, STC, or TSO process. This notice should be applied in conjunction with DO-178B, paragraph 2.5.

6. **THE USE OF EARLIER VERSIONS OF DO-178.** Versions of DO-178 earlier than revision B do not provide any guidance regarding FLS, and should not be used as a means of compliance for FLS approvals. For software developed to previous guidelines, at least the field-loadable component and the protective schemes of the component, should be demonstrated to meet the guidelines contained in DO-178B or an alternate means of compliance, as agreed to between the applicant and the cognizant ACO.

7. **APPROVAL OF FIELD-LOADABLE SOFTWARE (FLS).** The following procedures should be implemented as part of the TC, ATC, STC, or TSO process for the approval of FLS:

a. It should be confirmed that the software meets the objectives of DO-178B or another acceptable means of compliance, as agreed to between the applicant and the cognizant ACO.

b. It should be confirmed that the considerations outlined in DO-178B, paragraph 2.5, have been addressed.

c. It should be confirmed that the software and hardware configuration were verified/tested together during the verification process (i.e., the software must be installed on the target computer in which the approval was granted).

d. There should be a Configuration Management (CM) process in place to assure that the installation configuration (i.e., software part number, the hardware part number, the aircraft model, and the aircraft serial number combination, as applicable) is the same configuration that was approved during the TC, ATC, STC, or TSO process.

e. If redundant parts on the aircraft are field-loadable, the applicant should define the following: (1) the requirements for intermixing different software loads on the parts, (2)

requirements for partially successful and partially unsuccessful loads, and (3) the aircraft dispatchability effects of successful and unsuccessful loads on redundant parts.

f. There should be a process in place to assure that the software loaded is the software approved and that the software has not been corrupted (e.g., Cyclic Redundancy Check (CRC)). This process should include checks during product manufacturing, before installation onto the product, and after installation on the product.

NOTE 1: Per 14 CFR §21.1(b), a “product” is an aircraft, an aircraft engine, or an aircraft propeller.

NOTE 2: Different CRC algorithms give different assurances that the data transferred is correct. The applicant and approving authority should assure that the algorithm used is sufficient for the integrity required for the software level of the data being loaded.

g. If there is no process in place to assure that paragraph 7f above has been addressed, the airborne equipment to be field loaded should demonstrate compatibility with the onboard loading system during the verification process.

h. If there is no process in place to assure that paragraph 7f above has been addressed, the onboard loading system should be approved considering the following items:

(1) The applicant should demonstrate that the onboard loading system is in compliance with the guidelines of DO-178B, paragraph 2.5 or alternate means of compliance as described in Section 6 of this notice.

(2) The applicant should provide documentation defining the operation of the onboard loading system and the recommended means for maintaining configuration control of equipment by the operator. This documentation should include guidelines for the configuration control processes which meet the guidelines outlined in this notice.

(3) The applicant’s onboard loading system and procedures should be approved by the cognizant ACO. Depending on the implementation, this approval may include the data loader, as well as the procedures. (Note: Many approaches to data loading do not require evaluation of the data loader because integrity checks are built into the data and the data transfer process (see paragraph 7f of this notice).)

(4) If the applicant proposes more than one medium for onboard loading (e.g. diskette, mass storage, etc.), loading from all mediums should comply with the guidelines in this notice.

i. The applicant should demonstrate the ability to verify the airborne equipment software part number with onboard equipment, carry-on equipment, or other appropriate means.

j. Changes to FLS of software levels A or B, or equivalent software levels (e.g., DO-178A software level 1), should be reviewed and approved by the cognizant ACO.

k. Changes to FLS of software levels C, D, or E, or equivalent, should be coordinated with the cognizant ACO to assess any effects on the aircraft and to determine whether the changes are minor or major.

l. FLS which is also user-modifiable and has been approved by the cognizant ACO as user-modifiable does not require further determinations of compliance for dissemination and installation (reference DO-178B, paragraph 2.4).

8. INSTALLATION CONSIDERATIONS. The approved FLS may be installed on the aircraft via Service Bulletin, Engineering Change Request, or other FAA approved means. The approved means of installation varies, depending upon the method for granting approval. Whether the FLS approval is through TC, ATC, STC, TSO, or some other approval process, the document used to install the FLS should be approved by the cognizant ACO and should specify the following elements:

a. The aircraft and hardware applicability.

b. Verification procedures to assure that the software was correctly loaded into an approved and compatible target computer.

c. Any post load verification and/or test procedures required to show compliance to the guidelines specified in this notice.

d. Actions to be taken in the event of an unsuccessful load.

e. Reference to an approved loading procedure.

f. Maintenance record entry procedures required to maintain configuration control.

g. Reference to Aircraft Flight Manual, Aircraft Flight Manual Supplement, or Operator's Manual, as appropriate.

9. MAINTENANCE AND PART MARKING CONSIDERATIONS. Maintenance and part marking for FLS should be performed in accordance with the appropriate part of 14 CFR. Additional maintenance and part marking considerations that apply specifically to FLS using TC, ATC, STC, or TSO, process are discussed below:

a. The applicant's Aircraft Maintenance Manual (AMM) or Instructions for Continued Airworthiness (IFCA) should include the procedures to be followed when conducting maintenance on airborne equipment using field-loadable software.

b. The applicant's AMM or IFCA should include a procedure that requires maintenance personnel to verify the software part number configuration before and after maintenance is performed on the airborne equipment.

NOTE: If the software loading cannot be verified (e.g., procedures do not render proper results, checksum fails, part number does not match approved part number, etc.), the system should not be considered functional and the aircraft should not be dispatched. In some cases Minimum Equipment List (MEL) procedures may allow dispatch with some inoperative equipment. In the case of equipment whose software part number cannot be verified, the MEL should specify whether the affected equipment may be disabled and the aircraft subsequently returned to service. Other means to clear the aircraft for dispatch depend on the MEL limitations.

c. It is the responsibility of maintenance personnel to ensure the identified part is recorded in the necessary maintenance logs.

d. For airborne equipment having separate part numbers for hardware and software, the software part numbers need not be displayed on the outside of the unit, as long as it can be verified through some kind of electronic query. It is the maintenance personnel's responsibility to ensure that the software part identification has been logged. When new software is loaded into the unit, the same requirement applies and the approved software part number should be verified before the unit is returned to service.

e. For airborne equipment having only one part number, which represents a specific configuration of software and hardware, the unit identification on the nameplate should be changed when the new software is loaded. When new software is loaded, the software part number stored in the target computer after data loading should be verified electronically. It should be verified that the electronic software part number and the unit part number displayed on the nameplate are an approved configuration prior to returning the unit to service.

f. Changes to software part number, version, and/or operational characteristics should be reflected in the Operator's Manual, Aircraft Flight Manual, Aircraft Flight Manual Supplement, and/or any other appropriate document.

<<<Original signed by David W. Hempe on 11/18/98>>>

David W. Hempe
Acting Manager, Aircraft Engineering Division
Aircraft Certification Service

N8110.79 – Parts Manufacturer Approval (PMA) of Field-Loadable Software Notice

Appendix D

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.79

2/22/99

Cancellation
Date: 2/22/00

SUBJ: GUIDELINES FOR THE APPROVAL OF FIELD-LOADABLE SOFTWARE BY FINDING IDENTICALITY THROUGH THE PARTS MANUFACTURER APPROVAL PROCESS

1. PURPOSE. This notice provides guidelines to Federal Aviation Administration (FAA) Aircraft Certification Office (ACO) personnel, Manufacturing Inspection District and Satellite Office (MIDO/MISO) personnel, authorized Designated Engineering Representatives (DER), authorized Designated Manufacturing Inspection Representatives (DMIR), and authorized Designated Airworthiness Representatives (DAR) for approving field loadable software (FLS) using the Parts Manufacturer Approval (PMA) process for identicality. These guidelines are applicable to software data approvals related to type certificate (TC) approvals, amended type certificate (ATC) approvals, supplemental type certificate (STC) approvals, or Technical Standard Order authorizations (TSOA). This notice is for guidance purposes only and is supplemental to document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all ACOs, all Manufacturing Inspection Offices (MIO), all MIDOs and MISOs, and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Title 14 Code of Federal Regulations (14 CFR) part 21, "Certification Procedures for Products and Parts," §21.301, §21.303, and §21.305.

b. Advisory Circular 21-33, "Quality Assurance of Software Used in Aircraft or Related Products," dated February 3, 1993.

c. Advisory Circular 20-115, Revision B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

d. RTCA, Incorporated, document DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

e. FAA Order 8110.42, "Parts Manufacturer Approval Procedures," dated August 4, 1995.

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL),
A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220 (25
copies); AFS-600 (3 copies)

Initiated By: AIR-130

f. FAA Notice 8110.77, "Guidelines for the Approval of Field Loadable Software," dated November 18, 1998.

4. BACKGROUND.

a. Through technological advances, the loading of software in the field has become a common process. This process reduces aircraft down-time for maintenance and increases efficiency of maintaining airborne equipment.

b. To increase efficiency in accomplishing field loads, it has become desirable for the software developer to obtain approval in order to directly ship the software to the airline or operator. The current policy and guidance for PMA does not address FLS. Software does not fit the traditional concept of a part. The diskette, CD-ROM, etc. serves only as the media that carries a transformable representation of the software's executable image. The desired approval is not for the media, it is for the data on the media after it has been loaded into the target computer (i.e., the executable software itself). Since software does not fit the traditional definition for a part and has some unique considerations, this notice provides additional guidelines to use the PMA process for FLS.

c. This notice only addresses the PMA of FLS by identity. Due to its controversial nature and potential safety implications, PMA for FLS via the test and computation process is not addressed in this notice. This topic may be addressed in future policy. Should any issues regarding PMA of FLS via the test and computation process arise, please contact the software program manager in the AIR-130 branch at FAA Headquarters.

d. This notice does not address the development aspects of the FLS but focuses on the manufacturing and production issues for PMA of the FLS. Notice 8110.77 addresses guidelines for FLS development and approval and should be applied in conjunction with this notice.

5. PROCEDURES.

a. The PMA is used for replacement or modification parts for sale for installation on a type certificated product. Design approval using the PMA process may be accomplished in two ways: (1) By showing that the design is identical to a previously FAA approved design, or (2) By submitting test results and computations (data) showing that the design meets all applicable airworthiness requirements. As previously stated, this notice addresses the process for approving FLS using the identity approach. The test and computation approach is not addressed in this notice and may be addressed in future policy.

b. Establishing identity can be accomplished in one of two ways: (1) by showing evidence that the applicant obtained the design through licensing agreement, or (2) by comparing the applicant's design to a previously approved design. PMA for field loadable software should follow the same procedures as outlined in 14 CFR part 21 and FAA Order 8110.42, with the following additional considerations unique to software:

(1) Finding of identity by showing evidence of a licensing agreement.

a. Design Approval. Order 8110.42, paragraph 8(a)(3)(a) pertaining to licensing agreement states that the PMA applicant must show “documentation from the TC holder authorizing use of the submitted data package.” The following items should be considered for PMA design approval via the licensing agreement method:

(1) FLS to be approved via PMA should have been previously approved by the FAA through the TC, ATC, or STC process and should have the procedures in place discussed in Notice 8110.77.

(2) The approved software may be installed on the aircraft using a Service Bulletin or some other FAA approved means.

(3) There should be a configuration management process in place to assure that the combination of software part number, the hardware part number, the aircraft model(s), and the aircraft serial number(s), as appropriate, is the same combination that was approved during the TC, ATC, or STC process.

b. Design Changes. Order 8110.42, paragraph 8(h)(5) addresses the situation of design changes for PMA. For FLS that was approved via the PMA by showing evidence of licensing agreement, the following guidelines should be applied:

(1) Changes to FLS should be coordinated with the TC, ATC, or STC holder and cognizant ACO to assess if the effect of the change on the aircraft is major or minor. [Note: Major/minor change classification is described in 14 CFR, part 21, subpart D. Additional policy regarding the classification of major/minor software changes is being developed.]

(2) Paragraph 8(h)(5)(a) of Order 8110.42 states that major changes “must be substantiated and approved prior to implementation in the same manner as that for the original PMA.”

(3) If the change is determined to be minor, the procedure defined in Order 8110.42, paragraph 8(h)(5) should be followed.

(2) Finding of identity without a licensing agreement.

a. Design Approval. Order 8110.42, paragraph 8(a)(3)(b) states that the applicant’s identity statement must certify that the “design is identical in all respects to the design of the part covered under an approved design.” The following items should be considered for PMA design approval using identity without a licensing agreement:

(1) The FLS to be approved must be proven to be identical to software previously approved by the FAA through the TC, ATC, or STC process. [Note: The FLS originally approved as part of the TC, ATC, or STC process should have procedures in place as discussed in Notice 8110.77 and Section 12.5 of DO-178B.]

(2) Design identity may be demonstrated through some form of bit-by-bit check to demonstrate that the software is indeed the same.

(3) In addition to the bit-by-bit check, there should be design evidence available to support the identity claim. Evidence of design identity includes availability to all software development and design data required as part of the original approval. The data required by DO-178B or other acceptable means of compliance should be made available to the FAA to assure identity. This would include such items as software requirements data, design description, source code, executable object code, software configuration index, and software accomplishment summary, as listed in Section 9.4 of DO-178B. The presence of this design data is necessary to demonstrate that the software development process is identical and to support continued airworthiness concerns.

b. Design Changes.

(1) Design changes to FLS by identity without a licensing agreement should be considered major.

(2) Paragraph 8(h)(5)(a) of Order 8110.42 states that major changes “must be substantiated and approved prior to implementation in the same manner as that for the original PMA.”

c. The FAA and designee responsibilities for the PMA for FLS are the same as outlined in Order 8110.42 (i.e., the MIDO/MISO inspector or authorized DAR or DMIR address identity via licensing agreement; while the ACO engineer or authorized DER addresses other PMA approaches).

6. APPLICABILITY TO TSO. The applicability of the PMA to a unit containing FLS with TSO is the same as discussed in 14 CFR part 21 and Order 8110.42. If the PMA process is used for a unit with TSO containing FLS, it should follow the guidelines of this notice, in conjunction with 14 CFR part 21 and Order 8110.42.

7. CONCLUSION. The information and procedures described in this notice are meant to provide additional clarification and to promote consistent interpretation of the guidelines in DO-178B, Order 8110.42, and Notice 8110.77 for approving FLS by identity using the PMA process. This notice does not replace or supersede AC 20-115B, DO-178B, Order 8110.42, or Notice 8110.77.

<<Original Signed by James C. Jones on 2/22/99>>

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service

NOTES:

N8110.84 – User-Modifiable Software Notice

Appendix E

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.84

4/08/99

Cancellation

Date: 4/08/00

SUBJ: GUIDELINES FOR THE APPROVAL OF AIRBORNE SYSTEMS AND EQUIPMENT
CONTAINING USER-MODIFIABLE SOFTWARE

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," for approval of airborne systems and equipment designed to contain user-modifiable software components. These guidelines are applicable to the approval of airborne systems and equipment and the software aspects of those systems related to type certificates (TC), supplemental type certificates (STC), amended supplemental type certificates (ASTC), amended type certificates (ATC), and Technical Standard Order Authorizations (TSOA). This notice is for guidance purposes only and is supplemental to document DO-178B.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. DEFINITIONS.

a. **User-modifiable software**, as the term is used in DO-178B, is software intended for modification by the aircraft operator without review by the certification authority, the airframe manufacturer, or the equipment vendor, if within the modification constraints established during the original certification project. (Reference DO-178B, paragraph 2.4.)

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL),
A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220
(25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

NOTE: Modifications by the user to user-modifiable software may include modifications to data, modifications to executable code, or both, if within the modification constraints established during the original certification program.

b. Option-selectable software is software that contains approved and validated components and combinations of components that may be activated by the user, either through selection by the flight crew or activation by ground personnel. (Reference DO-178B, paragraph 2.4.)

c. Field-loadable software is software that can be loaded without removal of the equipment from the installation. Field-loadable software can refer to either executable code or data. (Reference DO-178B, paragraph 2.5.)

5. SCOPE. This notice applies to user-modifiable software only. The guidance provided below does not apply to option-selectable software nor field-loadable software, except where such software is also user-modifiable.

6. THE USE OF EARLIER VERSIONS OF RTCA/DO-178. Versions of DO-178 prior to version B did not provide any guidance regarding user-modifiable software, and should not be used as a means of compliance for user-modifiable software approvals. For software developed to previous guidelines, at least the user-modifiable component, the protective schemes, and any affected aspects of the non-modifiable component should be developed to DO-178B or other acceptable equivalent means as agreed to between the applicant and the ACO. DO-178B guidance for user-modifiable software is contained in Sections 2.4, 5.2.3, 7.2, 11.1, and 11.10 of that document. DO-178B also provides guidance for upgrading software from previous guidance in Section 12.1.4.

7. SAFETY CONSIDERATIONS.

a. User-modifiable software is software within an airborne system approved for user modification. Users (e.g., airlines, operators) may modify user-modifiable software within the specified modification constraints and with approved modification procedures without any further involvement by the certification authority. It is intended that once the system with the user-modifiable software has been certified, the certification authority should require no further visibility, review, or approval of modifications made to that user-modifiable software component. Therefore, modification of the user-modifiable software by the user should have no effect on the aircraft safety margins or operational capabilities, flight crew workload, any non-modifiable software components, or any protection mechanisms of the system.

b. An user-modifiable software component is that part of the software within the airborne system that is designed and intended to be changed by the user. A non-modifiable software component is one that is not designed or intended to be changed by the user. Any change that affects safety margins, operational capabilities, flight crew workload, any non-modifiable software components, protection mechanisms, or software boundaries, or that results in exceeding a

pre-approved range of data, parameters, or equipment performance characteristics warrants rescinding the classification of the software as user-modifiable, and requires design approval under the applicable regulations.

NOTE: Multiple trim values used as user-modifiable software that may affect safety require special attention. In general, it is not acceptable to simply test the trim value throughout its trim range, because of the uncertainty for acceptability of all the combinations of the trims. In most cases, it is not possible to verify all possible combinations of multiple trims. Therefore, in the case of multiple trims used as user-modifiable software, acceptance of verified sets of trims is generally required.

c. The potential effects of user-modifiable software modification must be determined by the system safety assessment and mitigated by system and software design means, development and verification assurance, approved procedures, and approved tools (if applicable). When evaluating data as part of the DO-178B process, the applicant and the approving FAA office should ensure that the protective mechanisms, verification, and user-modification procedures provide for non-interference of the non-modifiable components and protection integrity. The applicant should obtain the concurrence of the certification office early in the program as to the acceptability of the protective mechanism, protection verification, and modification procedures and tools.

NOTE: The purpose of the protective mechanism is to ensure that the user-modifiable component does not interfere with the non user-modifiable component. This protective mechanism should be evaluated during the initial approval of the system that contains user-modifiable software. It should be assured that no modification of the software by the user affects the protective mechanism. Section 10 of this notice will further address protection.

8. IDENTIFICATION OF DISPLAYED DATA. Where information is displayed to the flight crew and is derived from user-modifiable software, the information should be identified in such a way to indicate that it has not been approved by the certification authority. In the event that the design or inherent nature of the equipment or user-modifiable component makes the distinction between approved and unapproved information so readily apparent to the flight crew that errors distinguishing the two types of information are reasonably precluded, explicit identification may not be required. Such identification, where required, should be provided by the non-modifiable component and should allow the flight crew to readily distinguish between information approved by the certification authority and information not approved.

9. MODIFICATION OF AIRCRAFT PERFORMANCE PARAMETERS. An example of modifications that could affect the safety margins, operational capability of the aircraft, or crew workload include modifications of displayed data or other data provided to the flight crew for use in determining aircraft performance parameters. Modification of displayed data or other data provided to the flight crew for use in determining aircraft performance parameters requires

certification authority approval. Modification of the user-modifiable component to provide or revise these parameters, regardless of whether they are provided as primary or advisory information, requires certification authority approval. Such a change would warrant rescinding the classification of the software as user-modifiable and would require design approval and part number revision.

10. PROTECTION. Non-modifiable software components of the airborne system should be protected from user-modifiable software components. The system requirements should specify the protection mechanisms which prevent the user modification from affecting system safety, operational capability, or flight crew workload. If the system requirements do not include provision for user modification, the software should not be modified by the user. The protection mechanism should be assigned the assurance level associated with the most severe failure condition of the system as determined by the system safety assessment. If software provides the protection mechanism for user-modifiable software, that software protection should be assigned the highest software level of the system as determined by a system safety assessment. The protection should be such that any modification or failure of the user-modifiable software cannot result in loss of protection. Protection integrity cannot depend on any activities being accomplished by the user. The protection integrity should be such that it can neither be breached accidentally or intentionally. The applicant-provided means of modification of the user-modifiable software should be shown to be the only means by which the modifiable component can be changed.

11. TOOLS USED TO PROTECT NON-MODIFIABLE COMPONENTS.

a. DO-178B, Section 5.2.3, requires that the non-modifiable software components be protected from modifiable components in order to prevent interference with the safe operation of the non-modifiable software components. To enforce this protection, the use of the tools used to make the changes to the modifiable component is allowed. If such tools will be used to enforce this protection, then the following information should be provided to the certification authority for approval:

- (1) plans for controlling tool version;
- (2) plans for controlling tool usage;
- (3) plans for qualifying or verifying the tool; and
- (4) procedures for performing modifications to the tool.

b. Software forming a component of the tool and used in the protective function should be developed to the software level associated with the most severe failure condition of the system, as determined by a system safety assessment.

c. Use of software tools for user modifications requires tool qualification and approval of procedures of using and maintaining the tool. Changes to the tool or procedures may require re-qualification of the tool.

12. DATA REQUIREMENTS.

a. The applicant should identify in the Plan for Software Aspects of Certification (PSAC) their intention to develop an airborne system that will contain a user-modifiable software component(s). The PSAC should also describe the means of complying with DO-178B (including the design considerations of DO-178B Section 5.2.3), the protection mechanism, and the means of ensuring the integrity of the protection mechanisms. If software tools will be used for the modification, the PSAC should also identify tool qualification plans or verification procedures to ensure that the tool has modified the user-modifiable software to approved procedures and constraints and has not impacted the non-modifiable software or protection mechanisms.

b. The software design data should specify the design methods and details of implementation for ensuring protection from user modifications.

c. The Software Configuration Index should identify the approved procedures, methods, and tools for making modifications to the user-modifiable software, including tool qualification data, if applicable.

d. The Software Accomplishment Summary should summarize the entire development and verification of the non-modifiable software components, user-modifiable software component(s), protection mechanism, and modification procedures and tools, including tool qualification, if applicable.

13. OTHER CONSIDERATIONS. At the time of the user modification, the user assumes responsibility for all aspects of the user-modifiable software components and tools used for modifying the software, including software configuration management, software quality assurance, and software verification. User modifications should be performed to approved procedures established by the system requirements and software data using approved tools. If the user makes any modification to the non-modifiable software components, the protection mechanisms, the approved procedures, or the approved tools, other than those established by the system requirements and approved procedures; they have violated the type design, and the type certificate of the aircraft may be rescinded.

NOTE 1: During certification, the ACO should coordinate with that part of the regulatory authorities responsible for approving changes to the aircraft configuration in the field. This helps ensure the practicality and acceptability of the tools and procedures used to control the aircraft configuration.

NOTE 2: A system to track or log software modification that fall under the description in this notice should be considered where appropriate so that both the Certification and Continue Airworthiness aspects of the modifications may be reviewed by the cognizant authorities, as needed.

14. CONCLUSION. The information and procedures described in this notice promote clarification and consistent application the DO-178B guidance on the approval of airborne systems and equipment containing user-modifiable software. This notice does not replace or supersede AC 20-115B or DO-178B.

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service

N8110.78 – Approval of Software Changes in Legacy Systems Notice

Appendix F

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.78

12/07/98
Cancellation
12/07/99

GUIDELINES FOR THE APPROVAL OF SOFTWARE CHANGES IN LEGACY SYSTEMS USING RTCA DO-178B

1. PURPOSE. This notice provides guidelines to Aircraft Certification Service (AIR) field offices and to Designated Engineering Representatives (DER) regarding the application of RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," to software for systems that were developed prior the issuance of Advisory Circular (AC) 20-115B, "Radio Technical Commission for Aeronautics, Inc. Document RTCA/DO-178B," on January 11, 1993. These systems are referred to as legacy systems throughout this notice and refer to systems developed under DO-178 or DO-178A. AC 20-115B recognizes DO-178B as an acceptable means of compliance for the evaluation of software in airborne systems. DO-178B guidance for legacy systems is frequently misinterpreted and is not being consistently applied. This notice does not change the intent of DO-178B with regard to legacy systems but clarifies the application of DO-178B. Notice 8110.53, "Transition to RTCA/DO-178B, 'Software Considerations in Airborne Systems and Equipment Certification,'" was originally released to address this issue but did not meet all of the needs of the industry and certification authorities. This new notice should be used to apply DO-178B to legacy systems.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District and Satellite Offices (MIDO and MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B "Radio Technical Commission for Aeronautics, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

c. Notice 8110.53, "Transition to RTCA/DO-178B, 'Software Considerations in Airborne Systems and Equipment Certification,'" dated September 29, 1994.

A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL); A-FFS-7 (ALL); A-FFS-2, 8 (LTD);
AMA-220 (25 copies); AFS-600 (3 copies)

4. BACKGROUND. On January 11, 1993, the FAA issued AC 20-115B which recognizes DO-178B as a means to secure FAA approval of digital computer software. Prior to the issuance of AC 20-115B, many airborne systems were approved using DO-178 or DO-178A. These systems are referred to as legacy systems throughout this notice. Since AC 20-115B invokes DO-178B, many manufacturers are striving to use DO-178B on their legacy systems. There are several items to keep in mind when addressing the use of DO-178B on legacy systems:

a. DO-178B is different from the two previous versions of DO-178. The major change from the previous versions is the emphasis on a set of coordinated objectives rather than a collection of unrelated goal statements. There is also a change from an emphasis on documentation to a emphasis on objectives and the data needed to demonstrate compliance to those objectives. Software testing is the most visible difference between DO-178B and previous versions. Therefore, legacy systems approved under a previous version would not have the same level of testing assurance as that required by DO-178B (i.e., DO-178B clarifies the scope and extent of software testing and test coverage). AC 20-115B effectively cancels all previous versions of DO-178. Therefore, changes/modifications to systems accepted prior to the issuance of AC 20-115B or the migration of these systems to newer aircraft will be evaluated using DO-178B. Misinterpretations of the guidance of DO-178B regarding legacy systems have resulted in inconsistent application of the guidance, resulting in differences in efforts expended for similar changes. The issuance of Notice 8110.53 attempted to correct this problem but did not due to its inherent complexity.

b. Another difference between DO-178B and earlier versions is the classification of software levels and the need to perform a safety assessment to determine the software level. Previous versions only recognized three software levels, whereas DO-178B recognizes five software levels. There is no guidance that provides correspondence between these levels. This notice will provide a method to establish that correspondence. Once the correspondence has been established, then guidance provided by DO-178B may be applied to upgrade from a lower level to a higher level.

c. Prior versions of DO-178 do not address the qualification of tools. In many cases tools are involved in making changes to legacy systems. Therefore, modification projects for legacy systems are faced with the issue of how to address tools that were used and not evaluated as part of the original approval. The subject of tool qualification will not be specifically addressed in this notice but will be addressed in future policy.

d. After reviewing field experience with numerous changes, a procedure was developed to provide a more consistent approach to address changes to legacy systems. The approach described herein takes advantage of previous approvals while ensuring that changes are properly implemented and satisfy current FAA regulations and guidance. (Note: If the system contains multiple levels of software, the procedure should be applied to each of the partitioned sections that is affected by the change.)

5. DISCUSSION.

a. If the software level of the legacy system cannot be shown to be equivalent or better than that required by the installation being considered, then the software will have to be upgraded in accordance with procedures defined in DO-178B Section 12.1.4, "Upgrading a Development Baseline." This will require a complete reevaluation to demonstrate assurance to the appropriate objectives of DO-178B. Determining equivalence is addressed in Section 6 of this notice; however, application of DO-178B Section 12.1.4 is not addressed further in this notice.

b. There are four variables that can affect the actions needed in response to changes to legacy systems: (i) the assurance basis for original installation of the component containing the legacy software, (ii) whether DO-178B or previous version is the accepted means of assurance on the installation under consideration, (iii) whether the software is being modified or unchanged, and (iv) whether the software is being installed on the same or a different aircraft. Assuming that the software levels can be shown to be equivalent, the majority of legacy system issues of concern can be categorized into the following groups:

(1) Legacy systems software is not modified and is reinstalled on the original aircraft (to be addressed in section 6b of this notice).

(2) Legacy systems software is not modified but is installed on a different aircraft where DO-178B is not adopted as the means of demonstrating assurance (to be addressed in section 6b of this notice).

(3) Legacy systems software is modified and is reinstalled on the original aircraft (to be addressed in section 6c of this notice).

(4) Legacy systems software is modified and is installed on a different aircraft where DO-178B is not adopted as the means of demonstrating assurance (to be addressed in section 6c of this notice).

(5) Legacy systems software is modified and is installed on a different aircraft where DO-178B is adopted as the means of demonstrating assurance (to be addressed in section 6d of this notice).

(6) Legacy systems software is not modified but is installed on a different aircraft where DO-178B is adopted as the means of demonstrating assurance (to be addressed in section 6e of this notice).

c. Legacy systems, by definition, already have a recognized approval for installation or manufacturing through the Type Certificate (TC), Supplemental Type Certificate (STC), Amended Type Certificate (ATC), Technical Standard Order Authorization (TSOA), Production Certificate (PC), or Parts Manufacturer Approval (PMA) processes. If there are no changes to these systems, then the original approval of the software is still valid, assuming an equivalence to

the required software level can be ascertained (to be further discussed in Section 6 of this notice). Prior to installation in an aircraft, there should be some assessment that the systems are not going to be used in significantly a different manner than covered by the original installation approval. This notice does not address TSOA, since they are covered by Title 14 Code of Federal Regulations (14 CFR), Part 21, Subpart O and the governing Technical Standard Orders (TSO), as well as other policy from the Aircraft Certification Service Engineering Division (AIR-100). Although the information within this notice may be of use in evaluating changes to software-based products with TSOA, this notice was not written to address TSOA issues.

d. Systems with small, simple changes (e.g., gain changes where the new gain is within a band of gain settings originally tested, changes to maintenance information formatting, adding an additional output interface, changing data in a personality module that is within the original robustness test cases, etc.) should be handled as changes under the original approval basis (i.e., DO-178B does not need to be applied to the changes). The certification authority should be able to readily establish that these changes have been performed correctly under the original approval basis. The normal data submittals appropriate to the revision of DO-178 used for the original certification will still need to be evaluated to ensure that the changes are implemented correctly. If this cannot be done, then this is not a small, simple change. The determination of whether a change is small, simple cannot be made by objective considerations such as metrics or a count of lines of code. Therefore, this determination will be based on the individual judgment of the cognizant Aircraft Certification Office (ACO) Aviation Safety Engineer (ASE) or the Designated Engineering Representative (DER) making the evaluation (if the DER is delegated this authority).

Note: This process of allowing small, simple changes should not be followed, if the system is being used differently than the original certification project, or if the system has experience service difficulties.

e. When changes are made to legacy systems beyond the small, simple changes, assurance that the changes have been made properly will be required. The following items should be considered:

(1) Earlier versions of DO-178 do not contain well-defined acceptance criteria for a number of the requirements/guidelines. One example is in the area of testing. DO-178B requires that testing be sufficiently thorough to provide specific structural coverage criteria, whereas DO-178A only requires that testing exercise the logic but does not specify how extensively the logic be exercised.

(2) Additionally, some newer technologies and tool qualification are not even addressed in the earlier versions of DO-178. In all cases where ambiguities exist, the material in DO-178B will be used to provide a more exact interpretation.

(3) To be consistent with prior approvals, DO-178B should be used to evaluate the processes used to make the change, the changed software components, and those components affected by the software changes. Affected components should be identified by performing a change impact analysis of the software changes and identifying impacts on other components, interfaces, timing, memory, etc. (e.g., control coupling analysis, data coupling analysis, timing analysis, memory usage analysis, etc.). These analyses should also identify the level and extent of regression testing needed to verify the change.

(4) The unaffected portions of the software already have an approval basis and could be accepted in accordance with Section 5c of this notice. (It should be noted that the unaffected portion is the software that neither changed nor was affected by the change via control, data flow, or timing. The change impact analysis is used to determine the affected and unaffected portions.) In most cases, the risk of latent errors remaining in the software can be further mitigated by considering the benefit of service experience in conjunction with the prior approval. DO-178B Section 12.3.5, "Service Experience," contains a number of criteria that should be satisfied to allow the use of service experience. By virtue of the previous approval of the software, it may be assumed as already meeting the majority of the provisions of DO-178B Section 12.3.5. Little or no additional data should be required from the applicant regarding service experience under Section 12.3.5. (Note: The note in paragraph 12.3.5g of DO-178B does imply that additional data may be required to verify system safety objectives for software components and should be appropriately considered.)

(5) Once the change has been approved, the entire software should be considered to be assured to DO-178B at the appropriate software level. If the original assumption that service experience in conjunction with a prior approval was incorrect, then a number of field problems might surface. Since the process for changes has been assured to DO-178B standards, the subsequent changes will be addressed using DO-178B. Eventually, this may potentially result in the entire software being evaluated to DO-178B.

6. PROCEDURES. For any project involving changes to a legacy system or a different installation for a legacy system, the cognizant ACO ASE and/or DER should follow the procedures listed in this section.

a. The ASE and/or DER should establish that there is equivalence between the legacy system's software level(s) and the proposed installation's software level using Table 1 below. Table 1 illustrates the equivalence between DO-178/DO-178A and DO-178B. Table 1 is designed as a truth table asking the following question: "If the Legacy System has a specific DO-178/DO-178A software level, can it be installed on the product requiring a certain DO-178B level?" For example, if the legacy system has DO-178A/Level 2 software, it can be installed on a product requiring DO-178B Levels C, D, or E. There are two entries in Table 1 that may require analysis prior to determining equivalency; these instances are shown by an "Analyze" in Table 1. There should be an agreement between the ACO and applicant, when analysis is required.

If equivalency is not established by Table 1 (i.e., a "NO" entry in the table), the provisions of DO-178B Section 12.1.4 should be applied to upgrade the software level. Procedures for applying section 12.1.4 are not covered by this notice. The remainder of this notice assumes that equivalency has been established.

(Note: Per 14 CFR, Part 21, §21.1(b), a “product” is an aircraft, an aircraft engine, or an aircraft propeller.)

Table 1
Software Level Equivalence

DO-178B SW Level Required by the Installation	Legacy System Software Level per DO-178/DO-178A		
	<i>Critical/Level 1</i>	<i>Essential/Level 2</i>	<i>Non-essential/Level 3</i>
A	YES/Analyze	NO	NO
B	YES	NO/Analyze	NO
C	YES	YES	NO
D	YES	YES	NO
E	YES	YES	YES

b. If the legacy system’s software is unmodified and is being reinstalled on the same aircraft or a different aircraft where DO-178B is not required, then the original assurance process and associated data submittals may be accepted. This is only true if the system is being used in exactly the same way as originally certified, has no added functionality since the original certification, and has not experienced service difficulties (e.g., Airworthiness Directives, Service Bulletins, etc).

c. If the legacy system’s software is modified and installed on the same aircraft or on a different aircraft where DO-178B is not adopted as the means of demonstrating assurance, then either the assurance means of the original aircraft or the assurance means of the original legacy system may be used, providing the one with the latest revision is used.

d. If the legacy system software is modified and installed on different aircraft where DO-178B is adopted as the means of demonstrating assurance, it should be assessed if the change is a small, simple change (as discussed in Section 5d of this notice). Any changes determined to be small, simple changes may be handled the same as the not modified case discussed in Section 6b of this notice. The determination of whether a change is a small, simple change shall be at the discretion of the cognizant ACO ASE and/or DER. Some representative, but not exhaustive examples, of small, simple changes are given in Section 5d of this notice. If the changes is not a small, simple change, all the changes to the software and all of the components affected by the change should be assured using DO-178B (as discussed in Section 5e of this notice). The change impact analysis is the normal means of determining affected components. A description of change impact analysis is beyond the scope of this notice. However, the project plans and processes and the change activities and evidences should be shown to meet the objectives of

DO-178B. For example, if the original software was not evaluated using the structural coverage criteria in DO-178B Section 6 and Annex A, then DO-178B verification specified for the software level of the changed software will have to be done and coverage criteria satisfied. Additional affected, but unchanged, components may not have to be evaluated for logical structural coverage of the internal logic but would have to meet the requirements for data coupling and control coupling coverage (e.g., integration testing), as well as requirements-based test coverage for those affected functions. Once this process is complete, the applicant should be allowed to claim that their legacy system is now compliant with the guidelines of DO-178B.

e. If the legacy system software is not modified but is installed on a different aircraft (i.e., different type certificate) where DO-178B is adopted as the means of demonstrating assurance, then there should not be a separate assurance finding. The original approval serves as the installation approval of the software, unless the operational use of the system is expected to be significantly different (e.g., an air data computer installed on piston powered general aviation aircraft flying below 14,500 feet is now installed on a corporate jet flying at 50,000 feet). When the operational use is significantly different than the original certification basis, an assurance to DO-178B guidance should be performed. The determination of the significance in change of the operational use shall be at the discretion of the cognizant ACO ASE and/or DER (if the DER is delegated this authority).

f. All changes to legacy systems and the process used to approve those changes should be documented in the Plan for Software Aspects of Certification (PSAC), Configuration Index Document (CID), and/or the Software Accomplishment Summary (SAS), as appropriate for the specific project.

g. If any future changes are proposed, they should be addressed by using the criteria specified in this notice.

7. CONCLUSION. The information and procedures described in this notice are meant to provide additional clarification and to promote consistent interpretation of the guidelines in DO-178B for approving changes to software in legacy systems. This notice does not replace or supersede AC 20-115B or DO-178B.

<<Original signed by J.C. Jones on 12/7/98>>

James C. Jones
Manager, Aircraft Engineering Division,
Aircraft Certification Service

NOTES:

N8110.82 – Level D and Previously Developed Software Notice

Appendix G

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.82

3/26/99

Cancellation
Date: 3/26/00

SUBJ: GUIDELINES FOR APPLYING THE RTCA/DO-178B LEVEL D CRITERIA TO PREVIOUSLY DEVELOPED SOFTWARE (PDS)

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," to previously developed software (PDS) that has been categorized to contribute to at most a minor failure condition on the aircraft. Advisory Circular (AC) 20-115B recognizes DO-178B as an acceptable means of compliance for the evaluation of software in airborne systems and equipment. DO-178B assigns a software level of D to any software that can cause or contribute to no more than a minor aircraft failure condition. However, the application of the objectives associated with Level D software are frequently misinterpreted, especially when applied to software that was not originally approved using DO-178B (i.e., PDS). This notice should be used to apply DO-178B to PDS that is categorized as Level D.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District and Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the Federal Aviation Administration (FAA) Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. BACKGROUND. On January 11, 1993, the FAA issued AC 20-115B which recognizes DO-178B as a means of demonstrating compliance to regulations for the software aspects of aircraft systems. DO-178B provides for five different levels of software based on the software's contribution to potential failure conditions. These software levels represent differing levels of development process rigor based on the severity of the potential failure conditions to which the software can contribute. Level D is assigned to software that can cause or contribute to no more than a minor aircraft failure condition. DO-178B contains 28 objectives for Level D software that should be satisfied before approval is granted. To be consistent with a minor aircraft failure condition, the

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL);
A-FFS-7 (ALL); A-FFS-2,8 (LTD);
AMA-220 (25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

intent of Level D software objectives is to provide a thorough investigation of the functional behavior of the software and to provide the necessary configuration control. However, some of the required objectives for Level D have been misinterpreted when considered with the overall objective of establishing correct functional behavior. Due to confusion over Level D objectives, application of DO-178B for these systems has not been consistent over different projects. Many developers may decide to do more than the stated requirements for Level D; however, this notice concentrates on the minimum requirements. Proper application of Level D objectives permits the use of PDS, which is software that was not originally approved using DO-178B (e.g., Commercial-off-the-shelf (COTS) software, software developed using military standards, software developed using DO-178 or DO-178A, software developed using other industry standards). Reference Section 12.1 of DO-178B for additional guidance for using PDS. In particular, Section 12.1.4 should be referenced for additional considerations when upgrading a previous development baseline. While this notice addresses PDS, the guidelines may also be applicable for other software required to meet the DO-178B Level D objectives.

5. DISCUSSION. A consistent interpretation of DO-178B for Level D software is important for the approval of PDS software. Of the 28 objectives found in DO-178B for Level D software, experience has shown that there are five objectives that are frequently misinterpreted. One of the objectives is related to integral processes; the remaining four objectives are related to source code, software architecture, and low-level requirement definitions. The discussion presented in this section is applicable to any DO-178B, Level D, software approval. Section 6 provides specific procedures for the approval of Level D PDS.

a. Objective 1 in DO-178B, Annex A, Table A-1, "Software development and integral processes activities are defined." A number of field-experience comments point to the absence of any requirement to comply with Objective 6 in DO-178B, Annex A, Table A-1 which states "Software Plans comply with this document (i.e., DO-178B)" and have concluded that there should not be a requirement to comply with Objective 1 which states "Software development and integral processes activities are defined." However, Objective 1 ensures that even for Level D software: (1) there are some plans (e.g., Plan for Software Aspects of Certification, Software Development Plan, Software Configuration Management Plan, Software Quality Assurance Plan, Software Verification Plan), even if the plans themselves do not comply with DO-178B, and (2) those plans are followed (see Objective 1 in DO-178B, Annex A, Table A-9). Additionally, the plans should enable compliance to the DO-178B objectives applicable for Level D software.

b. Objective 4 in DO-178B, Annex A, Table A-2, "Low-level requirements are developed." For Level D software, the intent of this objective is to assure that the low-level requirements and architecture (software design) are defined. However, Table A-4 objectives related to the architecture and low-level requirements require no explicit verification of the software architecture and low-level requirements. Therefore, Objective 4 of Table A-2 is satisfied implicitly by satisfying Objectives 1 and 2 in DO-178B, Annex A, Table A-6. The satisfaction of Objectives 1 and 2 demonstrate that the executable code complies with and is robust with high-level requirements. Since there is no requirement to ensure that the executable code is compatible with the low-level requirements, it is not necessary to ensure that the low-level requirements are traceable to the high-level requirements.

c. Objective 3 in DO-178B, Annex A, Table A-2, “Software architecture is developed.” The logic as applied in paragraph 5(b) above may be applied to Objective 3 (i.e., Objective 3 is implicitly satisfied by other objectives and does not need to be explicitly satisfied for Level D PDS, since Table A-4, Objectives 8 through 12, do not require verification of the software architecture).

d. Objective 5 in DO-178B, Annex A, Table A-2, “Derived low-level requirements are defined” The referenced paragraph for Objective 5 (i.e., paragraph 5.2.1b) states that “Derived low-level requirements are provided to the system safety assessment process,” rather than just “defined.” As with the low-level requirements and software architecture, there is no explicit verification of derived low-level requirements for Level D software. The satisfaction of this objective is implied by satisfying Objective 2 in DO-178B, Annex A, Table A-2, “Derived high-level requirements are defined” and the associated verification of high-level requirements.

e. Objective 6 in DO-178B Annex A, Table A-2, “Source code is developed.” The actual DO-178B referenced text for Objective 6 (i.e., paragraph 5.3.1a) states, “Source code is developed that is traceable, verifiable, consistent, and correctly implements low-level requirements.” However, according to Annex A, Table A-5, there are no verification objectives for Level D source code. Therefore, there is no requirement to establish consistency between source code, low-level requirements, and high-level requirements. The consistency requirement is between the executable code and the high-level requirements for Level D. The objective is for the executable code to meet all of the functional verification elements. Furthermore, the existence of object code implies the existence of source code so that Objective 6 of DO-178B, Annex A, Table A-2 is reasonably covered by satisfying other objectives (i.e., Objectives 1 and 2 of Table A-2; Objective 2 of Table A-3; Objectives 1 and 2 of Table A-6; and Objective 3 of Table A-7) for level D software.

6. PROCEDURES. For a project involving approvals of Level D PDS, the cognizant ACO engineer and/or the DER (if authorized) should follow the procedures listed below:

a. Software reviewers should review the software plans to assure that: (1) some plans exist (e.g., Plan for Software Aspects of Certification, Software Development Plan, Software Configuration Management Plan, Software Quality Assurance Plan, Software Verification Plan); (2) those plans are followed (reference DO-178B, Annex A, Table A-9, Objective 1); and (3) the plans enable compliance to DO-178B objectives for Level D software.

b. Software reviewers can ensure that low-level requirements, software architecture, derived low-level requirements, and source code are defined and exist for Level D software; however, software reviewer should not assess the quality or compliance of these artifacts to DO-178B objectives and software life cycle data content requirements. The intent for Level D of these objectives will be satisfied by the objectives for Level D for Tables A-6 and A-7.

c. When evaluating the PDS, the following steps should be followed:

(1) The applicant should verify that a failure condition or malfunction of the Level D software can contribute to no more than a minor failure condition.

(2) The applicant should identify the functions to be used from the PDS.

(3) The applicant should ensure that the PDS can not result in an unacceptable failure condition in the target application.

d. In the case where multiple software levels for a given system and/or component exist, the protection and associated mechanisms between the different software levels should be verified to meet the objectives of the highest level of software associated with the system component. This can occur when there are multiple functions in a component (e.g., maintenance and navigation) or when there are different categorizations of types of failure conditions, such as loss of function versus a corrupted function (e.g., misleading display data). An example of the latter case is a navigation system supported by a PDS operating system. The loss of the navigation function can be shown to produce only a minor aircraft failure condition, whereas misleading navigation is usually considered to be a major aircraft failure condition. If the navigation function is protected (partitioned) from the operating system in such a way that any failure of the operating system can be shown to produce only a loss of function, then the operating system only needs to be evaluated to Level D criteria. However, the applicant needs to verify that indeed the operating system can only contribute to loss of navigation function and not to a misleading navigation failure condition. In this case, part of the development effort would be to demonstrate that the PDS can be shown to meet all the Level D objectives, as outlined above.

e. It is theoretically possible for Level D software to operate in conjunction with software of other levels. In this case a thorough protection/partitioning analysis should be performed in conjunction with the system safety assessment. However, discussion of protection/partitioning is outside the scope of this notice and will not be further discussed.

f. See DO-178B, Section 12.1, for additional guidance on the use of PDS.

7. CONCLUSION. The information and procedures described in this notice constitute a means to consistently interpret the guidelines in DO-178B for approving PDS that has been assessed to have a software level of D. The guidelines may also be applicable to other Level D software. This notice does not replace or supersede AC 20-115B or DO-178B.

<< Original Signed by James C. Jones >>

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service

N8110.83 – Software Tool Qualification Notice

Appendix H

NOTES:

NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.83

4/5/99

Cancellation

Date: 4/5/00

SUBJ: GUIDELINES FOR THE QUALIFICATION OF SOFTWARE TOOLS USING
RTCA/DO-178B

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and to Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," to the qualification of software verification and development tools. Advisory Circular (AC) 20-115B, "RTCA, Inc. Document RTCA/DO-178B," recognizes DO-178B as an acceptable means of compliance for securing the FAA's approval of software in airborne systems and equipment. Section 12.2 of DO-178B addresses tool qualification; however, the Section 12.2 criteria are often misinterpreted and result in inconsistent application in the field. This notice clarifies the application of DO-178B in the area of tool qualification but does not change the intent of DO-178B in this area. The guidelines in this notice should be used in applying the criteria in DO-178B for the qualification of tools.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. BACKGROUND. On January 11, 1993, the FAA issued AC 20-115B, which recognizes DO-178B as a means of demonstrating compliance to the regulations for the software aspects of airborne systems and equipment. Section 12.2 of DO-178B states that qualification of a tool is needed when processes in DO-178B "are eliminated, reduced, or automated by the use of a software tool, without its output being verified as specified in section 6" of DO-178B. DO-178B states, "The objective of the tool qualification process is to ensure that the tool provides

Distribution: A-W(IR)-3; A-X(CD)-4; A-FAC-0 (ALL),
A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220
(25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

confidence at least equivalent to that of the process(es) eliminated, reduced, or automated.” The items below provide further information regarding tool qualification:

a. Software development can be a very repetitive and human-labor intensive process. This can result in errors, as well as high costs. For these reasons various tools have been developed to automate portions of this process. If the tools are dependable, then improvements in productivity and lower numbers of in-service errors may be realized.

b. In order to certify systems developed by tools, the FAA, DERs, and applicants need to obtain confidence by qualification that these tools are dependable. DO-178B Section 12.2 was designed to provide criteria for establishing which tools require additional confidence and the criteria and data needed to establish that confidence. However, a number of provisions of this section are difficult to interpret. This notice provides a means to clarify the intent of DO-178B Section 12.2 and its application.

c. Some areas that have resulted in misinterpretation and inconsistent application of the DO-178B tool qualification criteria are:

- (1) When a tool should be qualified.
- (2) Justification for the different criteria for qualifying software development tools and software verification tools.
- (3) Which criteria apply to software development tools and which apply to software verification tools.
- (4) Data to be produced for software development tools and for software verification tools.
- (5) Acceptance criteria for tool operational requirements.
- (6) Tool determinism.
- (7) Tool partitioning assurance and evidence.
- (8) Tool configuration control.

d. These areas have resulted in inconsistencies in applying the criteria within DO-178B Section 12.2 to certification projects. This notice is designed to address the above problems by clarifying the intent and application of DO-178B Section 12.2.

5. DISCUSSION.

a. Not all software tools require qualification. According to DO-178B Section 12.2, qualification of a tool is needed only when processes described in DO-178B are eliminated, reduced, or automated by the use of that tool without its output being verified as specified in DO-178B Section 6. This means that if the results of the tool are being relied on to supply the sole evidence that one or more objectives are satisfied, the tool is required to be qualified per DO-178B Section 12.2. If the output of the tool is verified by some other means, then there is no need to qualify the tool. For example, if all the outputs of a test case generator are reviewed to ensure that coverage is achieved, then the tool does not need to be qualified. This notice provides guidelines to determine whether a particular tool requires qualification.

b. DO-178B Section 12.2 identifies two types of tools: software verification tools and software development tools. Each type will be discussed below.

c. DO-178B defines verification tools as "tools that cannot introduce errors, but may fail to detect them."

(1) The following are examples of verification tools:

a. A tool that automates the comparison of various software products (e.g., code, design) against some standard(s) for that product.

b. A tool that generates test procedures and cases from the requirements.

c. A tool that automatically runs the tests and determines pass/fail status.

d. A tool that tracks the test process and reports if the desired structural coverage has been achieved.

(2) Many claim that verification tools can be more reliable than humans in a number of verification tasks, if their correct operation is demonstrated. In order to encourage the use of verification tools, DO-178B Section 12.2 was designed to provide an acceptable approach to qualifying verification tools.

d. DO-178B defines development tools as "tools whose output is part of airborne software and thus can introduce errors." If there is a possibility that a tool can generate an error in the airborne software that would not be detected, then the tool cannot be treated as a verification tool. An example of this would be a tool that instrumented the code for testing and then removed the instrumentation code after the tests were completed. If there was no further verification of the tool's output, then this tool could have altered the original code in some unknown way. Typically, the original code prior to instrumentation is what is used in the product. This example is included to demonstrate that tools used during verification are not necessarily verification tools. The effect on the final product must be assessed to determine the tool's classification.

e. The reason for the distinction between development and verification tools is based on the likelihood of allowing an error into the airborne system. For development tools there is a potential to introduce errors directly into a system. However, a verification tool can only fail to detect an error that already exists in the product; therefore, a verification tool would need to be deficient in two different processes to allow an error to get into the airborne software: the development process introducing the error and the verification process to detect the error. For this reason, DO-178B calls for different levels of rigor in the qualification of verification and development tools.

6. PROCEDURES. For any project involving the qualification of tools, the ACO engineer and/or DER (if authorized) should follow the procedures and guidelines listed in this section:

a. Guidelines for determining whether a tool should be qualified:

(1) Whether a tool needs to be qualified is independent of the type of the tool (development or verification). There are three questions to ask to determine if a tool needs qualification. If the answer is “Yes” to all of the questions below, the tool should be qualified:

a. Can the tool insert an error into the airborne software or fail to detect an existing error in the software within the scope of its intended usage?

b. Will the tool’s output not be verified as specified in Section 6 of DO-178B?

c. Are processes of DO-178B eliminated, reduced, or automated by the use of the tool? That is, will the output from the tool be used to either meet an objective or replace an objective of DO-178B, Annex A?

(2) Once it has been determined that a tool does not require qualification, the remainder of DO-178B Section 12.2 is not applicable to that tool. In order to ensure timely response, the cognizant ACO engineer or DER (if authorized) should be involved early in the certification project’s tool qualification agreements.

(3) The Plan for Software Aspects of Certification (PSAC) should include a listing of all software tools and justification for why each tool does or does not require qualification.

b. Guidelines for determining which tool qualification criteria apply to development tools and which criteria apply to verification tools:

(1) Table 1 applies to tools requiring qualification and can be used to determine which criteria of DO-178B Section 12.2 apply to which type of tool. Table 1 shows the similarities and differences in the qualification criteria for development and verification tools. The column in Table 1 titled “Criteria” summarizes the DO-178B requirement; the column titled “Dev./Ref.” lists

the applicability of the criteria for development tools and the appropriate DO-178B section reference; and the column titled “Verif./Ref.” lists the applicability of the criteria for verification tools with the appropriate DO-178B section reference.

Criteria	Dev./Ref.	Verif./Ref.
Only deterministic tools may be qualified (to be further clarified in Section 6f of this notice).	Yes/12.2	Yes/12.2
Qualification should only be for a specific system; the intention should be stated in the PSAC.	Yes/12.2	Yes/12.2
Combined tools should be qualified to DO-178B, Section 12.2.1 unless partitioning can be shown (to be further clarified in Section 6g of this notice).	Yes/12.2.b	Yes/12.2.b
Software configuration management and software quality assurance process objectives should be applied to tools being qualified (to be further discussed in Section 6h of this notice).	Yes/12.2.c	Yes/12.2.c
Qualification should satisfy the same objectives as the airborne software.	Yes/12.2.1.a	No
The software level of the tool may be reduced.	Yes/12.2.1.b	No
A trial period may be used as a means of qualification.	Yes/ 12.2.1.c	Yes/12.2.2
Tool Operational Requirements should be reviewed.	Yes/12.2.1.d(1)	Yes/12.2.2
Compliance with Tool Operational Requirements under normal operating conditions should be demonstrated.	Yes/12.2.1.d(2)	Yes/12.2.2
Compliance with Tool Operational Requirements under abnormal operating conditions should be demonstrated.	Yes/12.2.1.d(3)	No
Requirements-based coverage should be analyzed.	Yes/12.2.1.d(4)	No
Structural coverage appropriate for the tool’s software level should be completed.	Yes/12.2.1.d(5)	No
Robustness testing appropriate for the tool’s software level should be completed.	Yes/12.2.1.d(6)	No
Potential errors should be analyzed.	Yes/12.2.1.d(7)	No

Table 1 – DO-178B Criteria Applicable to Tool Qualification

c. Guidelines for data submittal and data availability to demonstrate tool qualification. The requirements for data to support tool qualification are listed throughout DO-178B Section 12.2; however, there is no definitive guidance as to the minimum level/amount of data to be submitted to the FAA for tool qualification. The data submittals vary according to the type of tool being developed. Even though there are some similar requirements for the two tool types, the data requirements for each tool type are different. Table 2 summarizes the required tool qualification

data. The column titled “Data” lists the required data for tool qualification. The column titled “Applicability” summarizes if the data is applicable for development tool qualification (Development) or verification tool qualification (Verification). The column titled “Available/Submit” summarizes if the data should be submitted to the FAA or just available for FAA review. The column titled “DO-178B Ref.” lists the DO-178B section reference to the criteria. The remainder of this section discusses the tool qualification data summarized in Table 2.

Data	Applicability	Available/Submit	DO-178B Ref.
Plan for Software Aspects of Certification (PSAC)	Verification & Development (see Note 1 below)	Submit	12.2, 12.2.3.a, & 12.2.4
Tool Qualification Plan	Development Only (see Note 2 below)	Submit	12.2.3.a(1), 12.2.3.1, & 12.2.4
Tool Operational Requirements	Verification & Development	Available	12.2.3.c(2) & 12.2.3.2
Software Accomplishment Summary (SAS)	Verification & Development (see Note 1 below)	Submit	12.2.4
Tool Qualification Accomplishment Summary	Development Only (see Note 2 below)	Submit	12.2.3.c(3) & 12.2.4
Tool Verification Results	Verification & Development	Available	12.2.3.c
Tool Qualification Development data (e.g., design, code, test cases and procedures)	Development Only	Available	12.2.3.c

Table 2 – Data Required for Tool Qualification

Note 1: For development tool qualification, the PSAC should reference the Tool Qualification Plan and the SAS should reference the Tool Qualification Accomplishment Summary.

Note 2: The Tool Qualification Plan and the Tool Qualification Accomplishment Summary may be developed for verification tool qualification, if the applicant so desires.

(1) Verification Tool Qualification Data. Of the two tool qualification types, verification tools require the fewest data submittals and availability. Data for verification tool qualification are discussed below:

a. For verification tools, the applicant should specify the intent to use a verification tool in the PSAC (reference DO-178B, Section 12.2). The PSAC should be submitted to the FAA. This alerts the ACO engineer to provide a response to the intended use of the tool and opens a dialogue on acceptable qualification methods and documentation approaches. The ACO engineer and/or DER (if authorized) should provide written response to the applicant on the acceptability of the approach listed or referenced in the PSAC in a timely manner (i.e., the verification tool qualification approaches in the PSAC should be reviewed and approved or addressed in a timely manner).

b. For verification tool qualification, the Tool Operational Requirements should be documented and available to the FAA (reference DO-178B, Section 12.2.3.2). The requirements for the Tool Operational Requirements data are discussed in Section 6d of this notice.

c. Data that shows that all of the requirements in the Tool Operational Requirements have been verified should also be documented and available for FAA review. Sufficient verification data is needed to demonstrate normal operation only and will vary depending on the complexity of the tool, the purpose of the tool, and how the tool is used. This verification data may be packaged in any document deemed acceptable by the applicant.

d. An entry summarizing the results of the verification tool qualification should be included in the Software Accomplishment Summary (SAS). The SAS should be submitted to the FAA. This allows the ACO engineer to approve the results of the verification data and is evidence of the tool's qualification status.

Note: The applicant may choose to provide a separate Tool Qualification Plan and Tool Accomplishment Summary referenced by entries in the PSAC and the SAS for software verification tools. Entries are still required in the PSAC and SAS. This is an acceptable approach with the added benefit of providing the ability to reference a data package for reuse in subsequent certifications or in different certifications where the usage of the tool can be shown to be identical.

(2) Development Tool Qualification Data. There are additional requirements for a software development tool. The development tool data is similar to the requirements for the airborne software application development. For the software development tool qualification, the following data submittal and availability items should be considered:

a. For the development tool qualification, the actual qualification approach and data to be provided are specified in the Tool Qualification Plan. The Tool Qualification Plan should be submitted to and approved by the FAA.

b. The Tool Qualification Accomplishment Summary is also required for development tool qualification. It summarizes the results of the tool qualification process and describes and references the relevant tool qualification data. It should be submitted to and approved by the FAA.

c. For development tool qualification, the PSAC and SAS should be submitted to and approved by the FAA. However, these documents will likely only reference the Tool Qualification Plan and the Tool Qualification Accomplishment Summary documents.

d. For development tool qualification, the Tool Operational Requirements should be documented and available to the FAA (reference DO-178B, Section 12.2.3.2). The requirements for the Tool Operational Requirements data are discussed in Section 6d of this notice.

e. Data that shows that all of the requirements in the Tool Operational Requirements have been verified should also be documented and made available for FAA review. Sufficient verification data is needed to demonstrate normal operation and abnormal operation of the tool and will vary depending on the complexity of the tool, the purpose of the tool, and how the tool is used. This verification data may be packaged in any document deemed acceptable by the applicant.

f. Other tool qualification development data, such as design, code, test cases and procedures, etc. should be available for FAA review.

(3) The ACO engineer and/or DER (if authorized) should strive to use the document format and media used by the applicant for their own purposes. Any repackaging for submittal to the FAA should be undertaken only when the FAA is unable to review the data in any manner proposed by the applicant or the applicant is unable to meet the data retention provisions of the Federal Aviation Regulations.

d. Guidelines for evaluating acceptability of Tool Operational Requirements data: Tool Operational Requirements for any tool that requires qualification should be completed and made available for FAA review. A complete set of operational requirements is necessary to communicate to both the user and the reviewer what the tool does, how it is used, and the environment in which it performs. The Tool Operational Requirements must identify all functional and technical features of the tool and the environment in which it is installed (reference DO-178B, Section 12.2.3.2). The information required is different depending on the type of tool:

(1) For a verification tool, the Tool Operational Requirements should provide at least the following information:

a. The tool's functionality in terms of specific verifiable requirements that are verified as part of the tool's qualification testing.

b. A definition of the tool's operational environment, including operating system and any other considerations (e.g., an analysis of what tools will not do and what is required to cover that shortage (e.g., extensions to checklists, test cases) and any specialized hardware requirements (e.g., processors, special test equipment, or interfaces)).

c. Any other information necessary for the tool's installation or operation (e.g., User's Manual) should be included in the Tool Operational Requirements.

(2) A development tool needs to include all the information listed above for verification tools but should also include at least the following:

a. Software development processes performed by the tool.

b. Expected response under abnormal operating conditions.

Note: In some cases the User's Manual or other supplier's documentation may contain the needed information. Where additional information is included over and above the required information, the required information should be clearly identified. In the case where there is insufficient information from the tool supplier, the applicant should provide the missing information.

e. Guidelines on acceptable verification of the Tool Operational Requirements: Development and verification tools require verification of the Tool Operational Requirements. For verification tools, only verification over the normal operating conditions is required; whereas for development tools, verification over the abnormal operating conditions is also required. DO-178B Sections 6.4.2.1 and 6.4.2.2 describe verification for normal and abnormal conditions and will not be covered in this notice. However, since the operational requirements may contain additional information not directly related to the verification activity (e.g., the appearance of menus, dialog boxes, configuration), additional guidance is needed to reduce unnecessary verification for verification tools. For verification tools only, those portions of the operational requirements that are used directly in the setting up, conducting, monitoring, and reporting of verification need to be verified as part of tool qualification. The applicant should ensure that those features/portions of the verification tool that are not used have no adverse impact on those features/portions that are being used. If additional features are used at a later time, then additional verification will be required.

f. Guidelines on the interpretation of the determinism of tools:

(1) Although only deterministic tools can be qualified, the interpretation of determinism is often too restrictive. For example, some tools have graphical user interfaces that allow the user to interact in a diagrammatic fashion. Underlying these tools are data tables that capture the intended meaning of those diagrams. Often, however, the output from these tools is at least partially driven by the physical ordering of the entries in these data tables, and the ordering of the data table entries is not under the control of the tool user. It is possible to interpret the output of this kind of tool as being non-deterministic in the sense that apparently identical diagrammatic input could result in cosmetically (i.e., not functionally significant) different output from the tool. For example, a tool that generates compilable source code from flow chart diagrams might output the alternatives in a switch/case style construct in any one of many possible orders. Such a tool would not be allowed to be qualified under this interpretation of determinism.

(2) What is important is the ability to establish correctness of the output from the tool, not that the same apparent input necessarily leads to exactly the same output. If it can be shown that all possible variations of the output from some given input are correct under any appropriate verification of that output, then the tool should be considered deterministic for the purposes of tool qualification. This results in a bounded problem.

(3) This interpretation of determinism should apply to all tools whose output may vary beyond the control of the user, but where that variation does not adversely affect the intended use (e.g., the functionality) of the output and the case for the correctness of the output is presented. However, this interpretation of determinism does not apply to tools that have an effect on the final executable image embedded into the airborne system. The generation of the final executable image should be totally deterministic.

g. Guidelines for qualifying combined development and verification tools:

(1) The guidelines in this section apply only to tools which provide combined development and verification functions where the output of both the development and the verification functions are being used to eliminate, reduce, or automate processes of DO-178B. Combined tools that are used to eliminate, reduce, or automate only development objective(s) or only verification objective(s) should be qualified as such irrespective of the other capabilities present in that tool.

(2) Qualification of combined tools (when both the development and verification functions are being used to meet or replace objectives of DO-178B) should be performed to the guidance equivalent to the airborne software level ***unless protection/partitioning between the two functions can be demonstrated***. Acceptable evidence of this protection/partitioning would be to show that the output of one function of the tool has no effect on the output of the other function of the tool (i.e., the tool capabilities are functionally isolated).

(3) When protection/partitioning between the development and verification functions is shown, the protected/partitioned functions may be qualified as if they were separate development and verification tools (i.e., the verification functions may be qualified to the criteria for verification tools).

h. Guidelines on configuration management of qualified tools: In order to receive credit (i.e., meet or replace DO-178B objectives) for the use of qualified tools, those tools must be kept under configuration management. Not all of the requirements for configuration management of tools are contained in DO-178B Section 12.2. Section 12.2.3.b of DO-178B specifies the control categories for development and verification tool qualification data. DO-178B Section 7.2.9.b contains the requirement that software configuration management be applied to qualified tools.

i. Guidelines on verifying changes to previously qualified tools: A software change impact analysis should be conducted on all changes to tools that have been previously qualified. The analysis should be thorough enough to assess the impact of the tool change on the product, as well as other tools under the influence of the change. A regression analysis may form part of the change impact analysis.

j. Guidelines on DER approval of tool qualification data: If the ACO engineer has delegated compliance findings for tool qualification data, DERs may approve the tool qualification data which complies with the guidance of DO-178B, Section 12.2. However, approval of alternative methods and the resultant data should be retained by the ACO engineer.

7. CONCLUSION. The information and procedures described in this notice constitute a means to more consistently interpret the guidelines for tools qualified in accordance with the provisions of DO-178B, Section 12.2. This notice does not replace or supersede AC 20-115B or DO-178B.

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service

NOTES:

Appendix I

Course Evaluation Forms

There are two course evaluation forms in this Appendix. Please select the one appropriate for your method of study.

- IVT broadcast
- Self-study video course

If you are taking this course via IVT and you are logged on to a keypad, you will be asked to complete the course evaluation by using the Viewer Response System keypad. Your IVT instructor will provide directions on how to complete the course evaluation. If you do not have access to a keypad, circle your responses and fax the form to the IVT studio.

If you have completed this by watching the video, please complete the Self-Study Evaluation Form and return to your directorate/division training manager (ATM).

NOTES

IVT COURSE EVALUATION

Aircraft Certification's New Software Policy

April 28-29, 1999

Please give us your candid opinions concerning the training you've just completed. Your evaluation of the IVT course is important to us, and will help us provide the best possible products and services to you. **NOTE: Your keypad responses are not identifiable by name; only average item responses are provided to the instructor and to others responsible for the training.**

Use your Viewer Response keypad to answer the following questions.

	Very Good	Good	Average	Poor	Very Poor
1. Length of course	A	B	C	D	E
2. Depth of information	A	B	C	D	E
3. Pace of training	A	B	C	D	E
4. Clarity of objectives	A	B	C	D	E
5. Sequence of content	A	B	C	D	E
6. Quality of course materials	A	B	C	D	E
7. Quality of graphics/visual aids	A	B	C	D	E
8. Readability of text on monitor	A	B	C	D	E

SELF-STUDY VIDEO EVALUATION

Please give us your candid opinions concerning the training you've just completed. Your evaluation of the self-study video course is important to us, and will help us provide the best possible products and services to you.

Course title: _____

Date: _____

Number of years of FAA experience: _____

(Optional)Name: _____ Office phone: () _____

For the following, please darken the circle appropriate to your response.

	Very Good	Good	Average	Poor	Very Poor	N/A
1. Length of course	<input type="radio"/>					
2. Depth of information	<input type="radio"/>					
3. Pace of training	<input type="radio"/>					
4. Clarity of objectives	<input type="radio"/>					
5. Sequence of content	<input type="radio"/>					
6. Amount of activities/practice	<input type="radio"/>					
7. Quality of course materials	<input type="radio"/>					
8. Effectiveness of instructor(s)	<input type="radio"/>					
9. Overall quality of the course	<input type="radio"/>					
10. Overall effectiveness of the self-study video format	<input type="radio"/>					

11. Rate your level of knowledge of the topic before and after taking this self-study course.

	Very Low	Low	Moderate	High	Very High
BEFORE THE COURSE:	<input type="radio"/>				
AFTER THE COURSE:	<input type="radio"/>				

12. What did you like best about the course?

13. What would you improve in the course?

14. What previous experience, if any, have you had with self-study courses?

- None Moderate Considerable

15. Were you comfortable with the self-study video format?

- Yes No Undecided

If not, why not?

16. Would you like to take other self-study video courses?

- Yes No Undecided

If not, why not?

17. Additional comments:

**PLEASE SEND THIS COMPLETED FORM TO YOUR
DIRECTORATE/DIVISION TRAINING MANAGER (ATM). THANK YOU.**